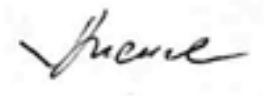
Государственное образовательное учреждение дополнительного образования детей
«Центр творческого развития и гуманитарного образования для одаренных детей «Поиск»

«УТВЕРЖДАЮ»
Директор Центра «Поиск»



А. В. Жигайлов
«11» января 2010 г.

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных государственного образовательного учреждения дополнительного образования детей «Центр творческого развития и гуманитарного образования для одаренных детей «Поиск»

Ставрополь, 2010

Оглавление

1. Общие положения

1.1. Данное Положение об организации и проведению работ по обеспечению безопасности персональных данных (далее по тексту – ПДн) при их обработке в информационных системах персональных данных (далее по тексту – ИСПДн) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящее Положение действует в Государственном образовательном учреждении дополнительного образования детей «Центр творческого развития и гуманитарного образования для одаренных детей «Поиск» (далее по тексту – Центр «Поиск»), расположенном по адресу: 355029, г. Ставрополь, ул. Мира, д. 460, и пяти его филиалах:

1) Кисловодский филиал Государственного образовательного учреждения дополнительного образования детей «Центр творческого развития и гуманитарного образования для одаренных детей «Поиск» (357700, Ставропольский край, г. Кисловодск, ул. Седлогорская, д. 1);

2) Изобильненский филиал Государственного образовательного учреждения дополнительного образования детей «Центр творческого развития и гуманитарного образования для одаренных детей «Поиск» (356140, Ставропольский край, г. Изобильный, пос. «Газопровод», МОУ СОШ № 23);

3) Невинномысский филиал Государственного образовательного учреждения дополнительного образования детей «Центр творческого развития и гуманитарного образования для одаренных детей «Поиск» (357100, Ставропольский край, г. Невинномысск, ул. Менделеева, д. 28);

4) Буденновский филиал Государственного образовательного учреждения дополнительного образования детей «Центр творческого развития и гуманитарного образования для одаренных детей «Поиск» (356800, Ставропольский край, г. Буденновск, пр-т Космонавтов, д. 1);

5) Минераловодский филиал Государственного образовательного учреждения дополнительного образования детей «Центр творческого развития и гуманитарного образования для одаренных детей «Поиск» (357200, Ставропольский край, г. Минеральные Воды, пр-т 22 Партсъезда, д. 94, ул. Пушкина, д. 57).

1.3. Положение определяет порядок работы персонала Центра «Поиск» (далее по тесту – пользователей) в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2. Порядок работы персонала в части обеспечения безопасности ПДн при их обработке в ИСПДн

Настоящий порядок определяет действия персонала Центра «Поиск» в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Допуск пользователей для работы с ПДн в ИСПДн осуществляется на основании приказа директора Центра «Поиск» о списке лиц, допущенных к работе в ИСПДн.

2.2. Пользователь в отведенное ему время осуществляет решение поставленных задач в соответствии с функциональными обязанностями и полномочиями доступа к ресурсам ИСПДн.

2.3. Пользователь несет ответственность за правильность эксплуатации автоматизированного рабочего места (далее – АРМ) и выполнения технических операций при работе в ИСПДн.

2.4. Вход пользователя в систему может осуществляться только по выдаваемому ему электронному идентификатору или по персональному паролю.

2.5. Запись информации, содержащей ПДн, может осуществляться пользователем на съемные электронные информационные носители, учтенные в Журнале учета электронных носителей.

3. Обязанности пользователя, участвующего в автоматизированной обработке ПДн в ИСПДн

Пользователь при работе в ИСПДн **обязан**:

3.1. соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

3.2. знать и выполнять правила работы со средствами защиты информации, установленными на АРМ (если такие имеются);

3.3. хранить в тайне свой пароль (пароли);

3.4. хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

3.5. выполнять требования Инструкции по организации антивирусной защиты в полном объеме;

3.6. известить руководителя структурного подразделения в случае:

- утери индивидуального устройства идентификации (ключа);
- подозрения компрометации личных ключей и паролей;
- обнаружения нарушений целостности АРМ или иных фактов совершения попыток несанкционированного доступа (далее по тексту – НСД) к защищенному АРМ;

− несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

− отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ, перебоев в системе электроснабжения;

− некорректного функционирования установленных на АРМ технических средств защиты;

− непредусмотренных отводов кабелей и подключенных устройств.

Пользователю при работе в ИСПДн категорически **запрещается**:

3.7. использовать компоненты программного и аппаратного обеспечения в неслужебных целях;

3.8. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн;

3.9. устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

3.10. осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

3.11. записывать и хранить конфиденциальную информацию на неучтенных электронных информационных носителях;

3.12. оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

3.13. оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, электронные информационные носители и распечатки, содержащие защищаемую информацию;

3.14. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации.

4. Порядок обеспечения работоспособности ИСПДн

Настоящий порядок определяет организацию резервирования информации, восстановления работоспособности технических средств, программного обеспечения и средств защиты информации в ИСПДн.

4.1. Пользователь ИСПДн, регламент работы которого предполагает осуществление резервного копирования информации, обязан осуществлять его не реже 1 раза в месяц.

4.2. Перед резервным копированием пользователь обязан проверить электронный информационный носитель на отсутствие вирусов.

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

4.4. Запрещается запись посторонней информации на электронные информационные носители, содержащие резервные копии.

4.5. Ответственность за проведение резервного копирования в ИСПДн возлагается на пользователя.

4.6. Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее – СЗИ) возлагается на программиста с функциями администратора сети, который обязан:

- знать перечень используемого в ИСПДН программного обеспечения (далее – ПО);
- производить необходимые настройки подсистемы управления доступом установленных в ИСПДН СЗИ от несанкционированного доступа и сопровождать их в процессе эксплуатации;
- реализовывать полномочия доступа для каждого пользователя к элементам защищаемых информационных ресурсов;
- своевременно корректировать полномочия доступа пользователей к защищаемой информации при изменении списка допущенных к работе лиц;
- проводить инструктаж пользователей по правилам работы с используемыми средствами защиты информации;
- осуществлять контроль порядка создания, учета, хранения и использования резервных копий массивов данных;
- настраивать и сопровождать системный журнал учета событий в ИСПДн, подлежащих регистрации;
- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в месяц;
- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;
- контролировать соблюдение пользователями порядка и правил проведения антивирусного тестирования;
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществлению несанкционированного доступа к защищаемой информации;
- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- в случае отказа средств защиты информации принимать меры по их восстановлению;

– докладывать заместителю директора по ИКТ о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

4.7. Заместитель директора по ИКТ обязан:

– разработать политику использования ПО в учреждении и следить за ее исполнением;

– разрабатывать плановые и распорядительные документы по организации защиты ПДн в соответствии с требованиями нормативных документов;

– организовывать и следить за выполнением мероприятий по защите информации;

– контролировать своевременное (не реже чем один раз в течение 180 дней) проведение смены паролей для доступа пользователей к АРМ;

– контролировать целостность печатей (пломб, защитных наклеек) на защищенных АРМ;

– требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических средств;

– требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

5. Порядок контроля защиты информации в ИСПДн

Контроль защиты информации в ИСПДн – комплекс организационных и технических мероприятий, которые осуществляются в целях предупреждения, пресечения или существенного затруднения возможности получения несанкционированного доступа к защищаемым ПДн, хищения технических средств и носителей ПДн, предотвращения воздействий, вызывающих нарушение целостности информации или работоспособности ИСПДн.

5.1. Основными задачами контроля являются:

– выявление демаскирующих признаков объектов ИСПДн;

– уточнение возможных каналов утечки защищаемой информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

– проверка выполнения установленных норм и требований по защите ИСПДн, оценка достаточности и эффективности мероприятий по защите информации;

– проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

– проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

– оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

– разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

5.2. Контроль защиты информации проводится с учетом реальных условий функционирования учреждения и осуществляется по объектовому принципу, при котором в учреждении одновременно проверяются все вопросы защиты информации.

5.3. В ходе контроля проверяются:

– соответствие принятых мер по обеспечению безопасности ПДн потенциальным угрозам защищаемой информации;

– своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по обеспечению безопасности ПДн;

– эффективность применения организационных и технических мероприятий по защите информации;

– устранение ранее выявленных недостатков,

– проведение необходимых измерений и расчетов приглашенными для этих целей специалистами органа по аттестации ИСПДн.

5.4. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее – предпосылка). По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований проводится расследование. Для проведения расследования назначается комиссия, которая должна установить, имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению.

5.5. Ведение контроля защиты информации осуществляется путем:

- проведения периодических проверок выполнения пользователями мероприятий по защите ИСПДн;
- обследования объектов ИСПДн (не реже одного раза в год).

5.6. Обследование объектов ИСПДн проводится с целью определения соответствия защищаемых помещений, основных и вспомогательных технических средств и систем требованиям по защите информации.

5.7. В ходе обследования проверяется:

– соблюдение организационно-режимных требований защищаемых помещений;

– сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений аппаратуры;

– наличие устройств непромышленного изготовления, которые могут способствовать возникновению каналов утечки информации;

– выполнение требований предписаний на эксплуатацию АРМ;

– выполнение требований по защите ИСПДн от несанкционированного доступа;

– выполнение требований по антивирусной защите.

6. Порядок проверки электронного журнала обращений к ИСПДн

Настоящий раздел Положения определяет порядок проверки электронного журнала обращений к ИСПДн.

6.1. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к конфиденциальной информации в ИСПДн.

6.2. Право проверки электронного журнала обращений имеет программист с функциями администратора сети.

6.3. В ИСПДн, где установлены средства защиты информации (далее – СЗИ), проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

6.4. В ИСПДн, где защита от несанкционированного доступа (далее – НСД) реализована организационно-распорядительными мероприятиями, проверка электронного журнала обращений проводится внутренними средствами операционной системы, при этом параметры «Доступ» и «Безопасность» настраиваются только в пользу программиста с функциями администратора сети.

7. Правила антивирусной защиты

Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного ПО, вирусов.

7.1. К использованию на АРМ допускаются только лицензионные антивирусные средства.

7.2. Установка и настройка средств антивирусного контроля на АРМ осуществляется программистом с функциями администратора сети.

7.3. Программист с функциями администратора сети осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

7.4. Заместитель директора по информатизации осуществляет ежегодное продление срока действия или закупку нового лицензионного антивирусного ПО.

7.5. После загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов АРМ.

7.6. Файлы, помещаемые в электронный архив, должны проходить антивирусный контроль.

7.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, программистом с функциями администратора сети должна быть выполнена антивирусная проверка ИСПДн.

7.8. На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

7.9. 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 самостоятельно (или вместе с администратором сети) должен провести внеочередной антивирусный контроль своего АРМ.

7.10. Организационное и техническое обеспечение процессов антивирусной защиты возлагается на программиста с функциями администратора сети.

7.11. Контроль проведения мероприятий антивирусной защиты осуществляет заместитель директора по информатизации.

8. Правила защиты паролей

Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей пользователей АРМ.

8.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на всех АРМ, обслуживающих ИСПДн, возлагается на программиста с функциями администратора сети, контроль действий осуществляет заместитель директора по информатизации.

8.2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями АРМ самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.);

– при смене пароля новое значение должно отличаться от предыдущего.

8.3. Полная плановая смена паролей пользователей должна проводиться не реже одного раза в течение 180 дней.

8.4. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий должна производиться программистом с функциями администратора сети немедленно после окончания последнего сеанса работы данного пользователя с системой.

8.5. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены и использования возлагается на заместителя по информатизации.

9. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе АРМ, обрабатывающих защищаемые ИСПДн.

9.1. Все изменения конфигураций технических и программных средств АРМ должны производиться только на основании заявок пользователей, ответственных за эксплуатацию конкретного АРМ.

9.2. Право внесения изменений в конфигурацию аппаратно-программных средств АРМ предоставляется работникам, функциональные обязанности которых предполагают обслуживание АРМ.

9.3. Изменение конфигурации аппаратно-программных средств АРМ кем-либо, кроме уполномоченных сотрудников, запрещено.

9.4. Процедура внесения изменений в конфигурацию системных и прикладных программных средств АРМ инициируется заместителем директора по информатизации, программистом с функциями администратора сети или заявкой пользователя АРМ.

9.5. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств АРМ:

– установка на АРМ программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн);

– обновление (замена) на АРМ программных средств, необходимых для решения определенной задачи;

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

9.6. Заявку рассматривает заместитель директора по информатизации, обозначая тем самым производственную необходимость проведения указанных в заявке изменений. После этого заявка передается ответственному лицу для непосредственного исполнения работ по внесению изменений в конфигурацию АРМ, указанного в заявке ИСПДн.

9.7. Если для обновления и модификации программного обеспечения защищаемых АРМ, требуется привлечение уполномоченных специалистов других учреждений (компаний), то работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

9.8. Установка и обновление ПО на АРМ производится только с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком или с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

9.9. После установки (обновления) ПО, ответственное лицо производит требуемые настройки средств управления доступом к компонентам АРМ, проверяет работоспособность ПО, правильность его настройки и производит соответствующую запись в «Журнале учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств АРМ».

9.10. При возникновении ситуаций, требующих передачи АРМ в ремонт, ответственный за его эксплуатацию докладывает об этом заместителю директора по информатизации. В данном случае ответственное лицо обязано предпринять необходимые меры для удаления защищаемой информации, которая хранилась на дисках компьютера.

9.11. Заявки должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств АРМ» у заместителя директора по информатизации.

9.12. Факт уничтожения защищаемых данных, находившихся на диске компьютера, оформляется актом за подписью заместителя директора по информатизации и ответственного лица.

9.13. С целью соблюдения принципа персональной ответственности за свои действия каждому работнику, допущенному к работе на АРМ конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и обрабатывать информацию в ИСПДн.

9.14. Использование несколькими работниками при работе на АРМ одного и того же имени пользователя ***запрещено***.

9.15. Процедура регистрации (создания учетной записи) пользователя и предоставления или изменения его прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн.

10. Порядок контроля соблюдения условий использования средств защиты информации

Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации.

10.1. Порядок работы с техническими СЗИ определен в соответствующих инструкциях, руководстве по настройке и использованию СЗИ, обязательных для исполнения как сотрудниками, обрабатывающими конфиденциальную информацию, так и администратором сети.

10.2. Право проверки соблюдения условий использования средств защиты информации имеют:

- заместитель директора по информатизации;
- назначенное ответственное лицо;
- программист с функциями администратора сети.

10.3. Пользователю ИСПДн категорически запрещается:

- обработка конфиденциальной информации с отключенными СЗИ;
- изменение настроек СЗИ.

10.4. Программисту с функциями администратора сети запрещается менять настройки программно-аппаратных СЗИ, предустановленных уполномоченными специалистами других организаций (компаний).

11. Порядок охраны и допуска посторонних лиц в защищаемые помещения

Настоящий раздел Положения устанавливает порядок охраны (сдачи под охрану) защищаемых помещений ИСПДн.

11.1. Вскрытие и закрытие помещений осуществляется работниками данных помещениях. Список работников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения, утверждается приказом директора Центра.

11.2. При отсутствии работников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, созданной на основании распоряжения директора Центра.

11.3. Заместитель директора по информатизации и администратор сети организуют проверку АРМ, ИСПДн на предмет несанкционированного доступа к конфиденциальной информации, наличия документов и машинных носителей информации о чём докладывается директору Центра.

11.4. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время оперативный дежурный сообщает о случившемся ответственному за помещение. Помещения вскрывать запрещается.

11.5. Помещения вскрываются ответственным в присутствии оперативного дежурного с составлением акта.

12. Заключительные положения

12.1. Требования настоящего Положения обязательны для всех работников, обрабатывающих защищаемую информацию.

12.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

12.3. Нарушения, связанные с выполнением требований руководящих документов по информационной безопасности, применению средств защиты информации и разграничению доступа, использованию технического, информационного и программного обеспечения ИСПДн, по степени их опасности делятся на нарушения первой, второй и третьей категории.

12.4. К нарушениям первой категории относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых сведений, утрату содержащих их электронных носителей информации и электронных документов, уничтожение (искажение) информационного и программного обеспечения, выведение из строя технических средств.

12.5. К нарушениям второй категории относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке) защищаемых сведений или утрате содержащих их электронных носителей информации и электронных документов, уничтожению (искажению) информационного и программного обеспечения, выведению из строя технических средств.

12.6. Остальные нарушения относятся к нарушениям третьей категории.