Приложение № 3

к приказу от 12.12.2022г. № 01-09-197

**ПОЛОЖЕНИЕ**

**об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации.**

**1. Общие положения.**

1.1. Данное «Положение об организации и проведении работ в КГБ ПОУ СГПТТ по обеспечению безопасности персональных данных при их автоматизированной обработке и/или без использования средств автоматизации в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы пользователей и ответственных за организацию работы по обработке ПНД с помощью информационных систем, ответственных за техническое обеспечение, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок создания резервных копий ИСПДн, правила хранения и регистрации носителей информации.

**2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации.**

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании трудового договора о приеме на работу, либо приказа, который издается директором КГБ ПОУ СГПТТ, и в соответствии со списком лиц, допущенных к работе в ИСПДн.

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей к информационным ресурсам определяются в матрице доступа, которая создается ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн и утверждается директором техникума.

2.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

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

2.5. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ в помещение, в котором производится обработка ПДн, аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и ***обязан***:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;

- хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли);

- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн о подозрении компрометации личных ключей и паролей, а также при обнаружении:

- иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным защищаемым СВТ;

- 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 СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на компьютеры технических средств защиты;

- непредусмотренных отводов кабелей и подключенных устройств.

2.8. Пользователю категорически ***запрещается***:

- использовать компоненты программного и аппаратного обеспечения персонального компьютера в неслужебных целях;

- вносить какие-либо изменения в конфигурацию аппаратных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

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

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (флеш-карты, ДВД-диски, ноутбуки и т.п.);

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

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

- размещать средства ИСПДн так, чтобы существовала возможность визуального считывания информации.

2.9. **Ответственный за организацию информационной безопасности** при их обработке в ИСПДн обязан:

- знать состав основных и вспомогательных технических систем, и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом: реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

 - вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;

- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

- проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

- контролировать своевременное (не реже чем один раз в течение 60 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;

- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в месяц;

- сопровождать подсистемы обеспечения целостности информации в ИСПДн;

- периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях.

- вести копии программных средств СЗИ от НСД и контролировать их работоспособность;

- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:

- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);

- участвовать в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

- вести учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн;

- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения;

- в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

- докладывать ответственному за обработку персональных данных в КГБ ПОУ СГПТТ о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

2.11. Ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн имеют право:

- требовать от сотрудников - 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 компонентов ИСПДн;

- 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, расследовании фактов несанкционированного доступа.

**3. Порядок обработки персональных данных без использования средств автоматизации.**

3.1. Обработка персональных данных без использования средств автоматизации может осуществляться в виде документов на бумажных носителях.

3.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

3.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

3.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

3.4.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

3.4.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

3.4.3. типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

3.4.4. типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

3.6. Ответственность за выполнение требований раздела 3 Положения возлагается на ответственных за обработку персональных данных (ОКиПР, бухгалтерии, по учебной работе).

**4. Порядок резервирования и восстановления работоспособности**

**технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации.**

4.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

4.2. Резервному копированию подлежат базы данных ПДн, а также прикладное программное обеспечение, предназначенное для работы с этими базами данных в случае, если оно подвергается модификации со стороны разработчиков ИСПДн.

4.3. Резервное копирование должно осуществляться в специально отведенный сетевой каталог на файловом сервере, а также путем записи на отчуждаемый носитель.

4.4. Права доступа к сетевым каталогам должны исключать возможность доступа пользователей к резервным копиям других ИСПДн, хранящихся на сервере, при отсутствии допуска к работе в этих ИСПДн.

4.5. Базы данных и программное обеспечение должны копироваться в разные папки на файловом сервере.

4.6. На файловом сервере, помимо актуального состояния баз данных и программного обеспечения, должны храниться минимум два их исторических состояния.

4.7. Раз в месяц ответственный за организацию безопасности обработки ПНд с помощью информационных систем ИСПДн создает резервную копию баз данных и программного обеспечения ИСПДн, хранящихся у ответственного за организацию безопасности обработки ПНд с помощью информационных систем, с ограничением доступа посторонним лицам.

4.8. К использованию, для создания резервных копий в ИСПДн, допускаются только зарегистрированные в журнале учета носители (если их копирование производится с их помощью).

4.9. Резервное копирование на файловый сервер должно осуществляться

непосредственно после любого изменения состояния баз данных или программного обеспечении этих баз.

4.10. Если программный продукт, на основе которого функционирует ИСПДн, имеет функцию резервного копирования, то администратор ИСПДн создает резервную копию при помощи данной функции.

4.11. Специалист, ответственный за техническое обеспечение учреждения создает резервную копию сетевого каталога, в котором хранятся резервные копии всех ИСПДн не реже чем раз в месяц.

4.12. Специалист, ответственный за техническое обеспечение учреждения, при помощи специализированного программного обеспечения, средств создает образы дисков всех рабочих мест ИСПДн не реже, чем раз в квартал.

4.13. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов либо полного восстановления системы с образа диска.

4.14. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

4.15. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

4.16. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

4.17. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств на зарегистрированный носитель.

4.18. Ответственность за проведение резервного копирования и копирования сетевого каталога хранения резервных копий ИСПДн ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн.

4.19. Мероприятия по восстановлению работоспособности технических средств и программного обеспечения баз данных организуются и проводятся специалистами, ответственными за техническое обеспечение учреждения, с привлечением ответственного пользователя той ИСПДн, функционирование которой было нарушено.

**5. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных.**

5.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации и продемонстрировать ответственному по информационной безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения под роспись в журнале учета пользователей, допущенных к информационным системам персональных данных.

5.2. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего положения, к работе в ИСПДн не допускаются.

5.3. Организация обучения и оказание методической помощи в КГБ ПОУ СГПТТ возлагается на ответственного за организацию информационной безопасности.

5.4. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций-лицензиатов ФСТЭК России и ФСБ России.

5.5. К работе в ИСПДн допускаются только работники, прошедшие первичный инструктаж по обеспечению безопасности в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в Журнале учёта допуска к работе в ИСПДн.

**6. Правила антивирусной защиты.**

6.1. На каждом компьютере ИСПДн должны быть установлены лицензионные антивирусные средства, сертифицированные ФСТЭК РФ.

6.2. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется специалистами, ответственными за техническое обеспечение информационных систем учреждения.

6.3. Специалисты, ответственные за техническое обеспечение информационных систем учреждения, осуществляют периодическое обновление антивирусных пакетов и контроль их работоспособности.

6.4. Установку и удаление средств антивирусной защиты также может осуществлять администратор информационной безопасности.

6.5. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

6.6. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

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

Настройку средств антивирусной защиты выполняет администратор информационной безопасности, либо специалисты, ответственные за техническое обеспечение учреждения, по согласованию ответственным за организацию информационной безопасности.

6.7. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

6.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором информационной безопасности должна быть выполнена антивирусная проверка ИСПДн.

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

6.10. 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 ответственным за организацию информационной безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов.

6.11. Организация антивирусного контроля в ИСПДн и проведение мероприятий антивирусной защиты в конкретной ИСПДн. в соответствии с требованиями настоящего Положения возлагается на ответственного за организацией информационной безопасности, при этом ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн ьакже возлагается и на всех пользователей данной ИСПДн..

**7. Правила парольной защиты.**

7.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

7.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на ответственного за организацией информационной безопасности.

7.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями объекта вычислительной техники 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 (@, #, $, &, \*, % и т.п.);

- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

- при смене пароля новое значение должно отличаться от предыдущих;

- пользователь не имеет права сообщать личный пароль другим лицам.

7.4. В случае имеющейся служебной необходимости, продиктованной возникновением нештатных ситуаций или других форс-мажорных факторов, при условии отсутствия на рабочем месте пользователя ИСПДн, руководитель структурного подразделения КГБ ПОУ СГПТТ оформляет в письменном виде заявку на сброс пароля отсутствующего пользователя и направляет ее ответственному за организацию безопасности персональных данных при их обработке в ИСПДн. В заявке должно быть изложено обоснование необходимости сброса пароля, указаны Ф.И.О. пользователя, чей пароль необходимо сбросить, Ф.И.О., должность специалиста, который будет осуществлять обработку ПДн от имени отсутствующего пользователя, а также временной отрезок, в течение которого им будет производиться обработка ПДн.

7.5. После выполнения необходимых работ все пароли изменяются и передаются пользователям ИСПДн. После этого пользователи устанавливают себе новые пароли.

7.6. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 60 дней.

7.7. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться ответственным за организацию информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой на основании сообщения руководителя структурного подразделения КГБ ПОУ СГПТТ.

7.8. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) ответственного за организацию информационной безопасности.

7.9. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

7.10. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на ответственного за организацию информационной безопасности.

**8. Правила обновления и конфигурирования программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн.**

8.1.Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления и конфигурирования программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн.

8.2. Все изменения программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн, должны производиться ответственным за организацию информационной безопасности и/или лицами ответственными за техническое обеспечение КГБ РОУ СГПТТ (при согласовании с ответственным за организацию информационной безопасности), с одновременным уведомлением ответственного в КГБ ПОУ СГПТТ за обработку персональных данных.

8.3. Обновление и конфигурация программного обеспечения, не используемого для непосредственной обработки ПДн и не являющегося ПО СЗИ, а также аппаратной составляющей элементов ИСПДн, осуществляется сотрудниками технического обеспечения в обычном порядке.

8.4. В случае если АРМ проходил аттестацию соответствия требованиям защиты информации, изменение аппаратно – программной составляющей ИСПДн производится на основании заявки.

8.5. Изменение конфигурации программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников ***запрещено***.

8.6. Процедура внесения изменений в конфигурацию программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн, инициируется заявкой ответственного за организацию работы по информационной безопасности ИСПДн.

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

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн);

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

- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

8.8. Заявку, в которой требуется произвести изменения конфигурации, рассматривает директор ГКБ ПОУ СГПТТ, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений, после чего заявка передается ответственному за организацию информационной безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке самостоятельно или с привлечением сотрудников, ответственных за техническое обеспечение учреждения.

8.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором информационной безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного по организации контроля информационной безопасности ИСПДн.

8.10. Установка или обновление подсистем ИСПДн должны проводиться в соответствии с технологией проведения модификаций программных комплексов данных подсистем, указанной в технической документации, если таковая имеется.

8.11. Установка и обновление ПО (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт-дисков и т.п.), прикладного ПО – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

8.12. ПО средств защиты информации устанавливается с носителей, обладающих специальной голографической наклейкой, подтверждающей их подлинность, если иное не указано в документации к данному ПО.

8.13. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также на совместимость с установленными программным обеспечением и операционной системой.

8.14. После установки (обновления) ПО, администратор информационной безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера, проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки, модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте» (при наличии).

8.15. Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» устанавливается приказом директора КГБ ПОУ СГПТТ.

8.16. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн, который обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн.

8.18. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью ответственного за организацию информационной безопасности и сотрудника, ответственного за техническое обеспечение (техник-программист).

**9. Управление учетными записями пользователей.**

9.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должна быть создана уникальная учетная запись пользователя.

9.2. Работу в ИСПДн сотрудник должен осуществлять только с использованием своего уникального имени пользователя. Работа в ИСПДн под чужой учетной записью, кроме случаев, описанных в п.7.4, ***запрещена.***

9.3. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 60 дней.

9.4. После внесения изменений в списки пользователей ответственный за организацию информационной безопасности должен обеспечить настройки средств защиты, соответствующие требованиям безопасности, указанной ИСПДн.

**10. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических.**

10.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

10.2. Технические средства защиты информации являются важным компонентом ОБ ПДн.

10.3. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками, обрабатывающими конфиденциальную информацию, так и ответственным за организацию информационной безопасности.

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

- директор техникума;

- ответственные за обработку персональных данных;

- ответственный за организацию информационной безопасности.

10.5. Пользователю ИСПДн категорически запрещается:

- отключать СЗИ;

-производить обработку конфиденциальной информации в случае неработоспособности средств ее защиты (СЗИ);

- менять настройки СЗИ.

10.6. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено несанкционированное изменение конфигурации программных средств ИСПДн об этом докладывается ответственному за обработку ПНд с последующим докладом директору КГБ ПОУ СГПТТ.

10.7. Криптографические средства защиты информации должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

**11. Порядок охраны и допуска посторонних лиц в защищаемые помещения.**

11.1. Данный раздел Положения устанавливает порядок охраны помещений ИСПДн.

11.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

11.3. При отсутствии сотрудников, ответственных за вскрытие помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа. Комиссией составляется акт вскрытия.

11.4. При закрытии помещений сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убирают для хранения в опечатываемый сейф (металлический шкаф).

11.5. Постановка и снятие помещений под охрану производится сотрудником ЧОО, либо лицом, из списка работников, утвержденных директором КГБ ПОУ СГПТТ после окончания и перед началом рабочего дня соответственно.

11.6. Сотрудник, имеющий право на вскрытие помещений:

- вскрывает помещение.

11.7. При обнаружении повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии сотрудника ЧОО. О происшествии немедленно сообщается директору техникума и (или) ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн.

Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

11.8. Ответственный за обработку ПНд в КГБ ПОУ СГПТТ и ответственный за организацию информационной безопасности организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

11.9. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время сотрудник ЧОО сообщает о случившемся директору КГБ ПОУ СГПТТ, и/или ответственному за помещение. Помещения вскрывать запрещается.

11.10. Помещения вскрываются ответственным за помещение, или директором техникума, или ответственным за обработку ПНд в присутствии сотрудника ЧОО с составлением акта.

11.11. Порядок пребывания посторонних лиц на территории КГБ ПОУ СГПТТ

устанавливается соответствующим приказом.

**12. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации.**

12.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

12.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

12.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

12.4. Бумажные и прочие сгораемые носители уничтожают путем сжигания или с помощью любых бумагорезательных машин.

12.5. По факту уничтожения или стирания носителей составляется акт, который утверждается ответственным за обработку ПНд в КГБ ПОУ СГПТТ. в журналах учета делаются соответствующие записи.

12.6. Процедура стирания и уничтожения осуществляются комиссией, в которую входят:

- ответственный за организацию информационной безопасности, техник-программист,

- ответственный за обработку ПНд, в структурном подразделении которого, происходит данная процедура (ОК и ПР, бухгалтерия, по учебной работе).

**13. Обезличивание персональных данных.**

13.1. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных

13.2. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

13.3. Способы обезличивания при условии дальнейшей обработки персональных данных:

- метод введения идентификаторов;

- метод изменения состава или семантики;

- обобщение (понижение точности некоторых сведений);

- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;

- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

13.4. Для обезличивания персональных данных используются способы обезличивания, определенные приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» в соответствии с рекомендациями по использованию этих методов.

13.5. Решение о необходимости обезличивания персональных данных принимает директор КГБ ПОУ СГПТТ по предложению ответственных за обработку ПНд (ОКиПР, бухгалтерии, по учебной работе) и обосновав такую необходимость и способ обезличивания.

13.6. Работники структурных подразделений, обслуживающих базы данных с персональными данными, осуществляют непосредственное обезличивание выбранным способом.

13.7. Порядок работы с обезличенными персональными данными:

13.7.1. Обезличенные персональные данные не подлежат разглашению.

13.7.2. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

13.7.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;

- антивирусной политики;

- правил работы со съемными носителями (если они используется);

- правил резервного копирования;

- правил доступа в помещения, где расположены элементы информационных систем;

13.7.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;

- правил доступа к ним и в помещения, где они хранятся

Приложение

ТИПОВАЯ ФОРМА

журнала учета машинных носителей информации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Регистрационный (учетный) номер носителя | Вид носителя | Тип носителя и его емкость | Дата поступления |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Расписка в получении (ФИО, подпись, дата) | Расписка в обратном приеме (ФИО, подпись, дата) | Место хранения | Дата и номер акта об уничтожении | Примечание |
| 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |

ТИПОВАЯ ФОРМА

журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Дата | Краткое описание выполненной работы (нештатной ситуации) | ФИО ответственного за безопасность в ИСПНд (исполнителя) и их подписи |
| 1 | 2 | 3 | 4 |
|  |  |  |  |

|  |  |
| --- | --- |
| ФИО ответственного за эксплуатацию ПЭВМ, подпись | Примечание (ссылка на заявку) |
| 5 | 6 |

ТИПОВАЯ ФОРМА

журнала учета пользователей, допущенных к информационным системам персональных данных

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Дата | Фамилия, имя, отчество пользователя | Наименование ИСПДн |
| 1 | 2 | 3 | 4 |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Подпись пользователя об ознакомлении с Положением и требованиями по безопасности | Подпись администратора безопасности о готовности пользователя к работе в ИСПДн | Примечание |
| 5 | 6 | 7 |
|  |  |  |