

**(ГАПОУ СО «ИПТ»)**

**ПРИКАЗ**

от 25.12.2015 г.

№ 229

г. Ирбит

**Об утверждении «Положения об организации и проведении работ в ГАПОУ СО «Ирбитский политехникум» по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных»**

Во исполнение Постановления Правительства Российской Федерации № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также прочих нормативных документов по защите информации

**П Р И К А З Ы В А Ю:**

1. Утвердить «Положение об организации и проведении работ в ГАПОУ СО «Ирбитский политехникум» по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных» (Приложение 1).
2. Утвердить типовые формы журналов:
  - Журнал поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним (Приложение 2);
  - Журнал учета машинных носителей (Приложение 3);
  - Журнал учета хранилищ (Приложение 4);
  - Журнал периодического тестирования средств защиты информации (Приложение 5);
  - Журнал учета нештатных ситуаций в работе информационных систем персональных данных, выполнении профилактических работ, установки и модификации программных средств на компьютерах информационных систем персональных данных (Приложение 6);
  - Журнал учета пользователей, допущенных к работе в информационных системах персональных данных (Приложение 7).




*Котто Верна*      *Ирбит*      *25.12.2015*      *Н.Н. Мурадылова*

- Журнал учета проверок электронных журналов (Приложение 8).
3. Завести журналы согласно типовых форм и ведение журналов возложить на должностных лиц согласно их обязанностям.
  4. Контроль за исполнением настоящего приказа оставляю за собой.

Приложения:

1. Положение об организации и проведении работ в ГАПОУ СО «Ирбитский политехникум» по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных;
2. Типовая форма журнала поездочного учета средств защиты информации, эксплуатационной и технической документации к ним;
3. Типовая форма журнала учета машинных носителей;
4. Типовая форма журнала учета хранилищ;
5. Типовая форма журнала периодического тестирования средств защиты информации;
6. Типовая форма учета нештатных ситуаций в работе информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационных систем персональных данных;
7. Типовая форма журнала учета пользователей, допущенных к работе в информационных системах персональных данных;
8. Типовая форма журнала учета проверок электронных журналов.

Директор

 / Н.Н. Журавлева /



Приложение 1 к Приказу  
ГАПОУ СО «Ирбитский  
политехникум»  
от «25» декабря 2015 г. № 229

***Положение об организации и проведении работ в ГАПОУ СО «Ирбитский политехникум» по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных***

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Данное «Положение об организации и проведению работ в ГАПОУ СО «Ирбитский политехникум» по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 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 персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к 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 охраны и допуска посторонних лиц в защищаемые помещения.

**2. ПОРЯДОК РАБОТЫ ПЕРСОНАЛА ИСПДН В ЧАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДН ПРИ ИХ ОБРАБОТКЕ В ИСПДН**

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

2.2. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа, который издается руководителем ГАПОУ СО «Ирбитский политехникум» (далее руководитель), и в соответствии со списком лиц, допущенных к работе в ИСПДн. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн руководителем назначается администратор безопасности, с целью контроля выполнения необходимых мероприятий по обеспечению безопасности ответственный за защиту информации.

2.3. 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, утверждаемой руководителем организации. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в «Журнале учета машинных носителей».

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

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

2.6. Запись информации, содержащей ПДн, может, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в «Журнале учета машинных носителей».

2.7. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.8. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к 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);
- хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
- выполнять требования Положения по организации антивирусной защиты в полном объеме.

2.9. Немедленно известить ответственного за защиту информации и (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или 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.

2.10. Пользователю категорически **запрещается**:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных 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 (гибких магнитных дисках и т.п.);
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было 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 с них существовала возможность визуального считывания информации.

2.11. Администратор безопасности (а при его отсутствии – ответственный за защиту информации) 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:

- 1) реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

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

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

- контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;

- 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 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;

- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в 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 описание событий, подлежащих регистрации в системном журнале;
- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 10 дней;
- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации, и учета бумажных носителей информации. 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 две копии программных средств СЗИ от НСД и контролировать их работоспособность;
- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;
- 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;
- сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;
- контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;
- 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);
- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- вести «Журнал учета нештатных ситуаций в работе информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационных систем персональных данных»;



- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положений в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- докладывать ответственному за защиту информации, ответственному за эксплуатацию ИСПДн о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.12. Администратор безопасности и ответственный за защиту информации 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 и расследования фактов несанкционированного доступа.

### **3. ПОРЯДОК РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ, ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

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

3.2. К использованию, для создания резервной копии в ИСПДн, допускаются носители, только зарегистрированные в «Журнале учета машинных носителей».

3.3. Администратор безопасности **обязан** осуществлять периодическое резервное копирование конфиденциальной информации.

3.4. Еженедельно, по окончании работы с конфиденциальными документами (содержащими персональные данные) на компьютере, пользователь, при отсутствии администратора, обязан создавать резервную копию конфиденциальных документов на зарегистрированный носитель (ЖМД, ГМД, CD, DVD – диски, USB накопитель, другие), создавая тем самым резервный

электронный архив конфиденциальных документов.

3.5. Носители информации (ЖМД, ГМД, CD-ROM, USB накопитель, другие), предназначенные для создания резервной копии и хранения конфиденциальной информации выдаются установленным порядком руководителем, ответственным за защиту информации и(или) администратором. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности, или руководителю, или ответственному за защиту информации.

3.6. Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель) на отсутствие вирусов.

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

3.8. Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD-ROM, USB накопитель и другие) резервной копии.

3.9. Порядок создания резервной копии:

- вставить в компьютер зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;
- выбрать необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполнить процедуру создания резервной копии;
- произвести копирование на отчуждаемый носитель;
- произвести отключение отчуждаемого носителя и, создав не обходимые записи в журналах убрать носитель в хранилище.

3.10. Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

3.11. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

3.12. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

3.13. При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором безопасности, ответственным за защиту информации и, при условии проведенной аттестации информационной системы, представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. 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.

3.14. 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.

3.15. 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. Настройку данных средств должен выполнять сотрудник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

3.16. 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 с помощью встроенных в них функций на зарегистрированный носитель.

3.17. Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности.

3.18. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

3.19. Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее – СЗИ) возлагается администратора безопасности.

#### **4. ПОРЯДОК КОНТРОЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИСПДН И ПРИОСТАНОВКИ ПРЕДОСТАВЛЕНИЯ ПДН В СЛУЧАЕ ОБНАРУЖЕНИЯ НАРУШЕНИЙ ПОРЯДКА ИХ ПРЕДОСТАВЛЕНИЯ. ПОРЯДОК РАЗБИРАТЕЛЬСТВА И СОСТАВЛЕНИЯ ЗАКЛЮЧЕНИЙ ПО ФАКТАМ НЕСОБЛЮДЕНИЯ УСЛОВИЙ ХРАНЕНИЯ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИСПОЛЬЗОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ПРИНЯТИЕ МЕР ПО ПРЕДОТВРАЩЕНИЮ ВОЗМОЖНЫХ ОПАСНЫХ ПОСЛЕДСТВИЙ**

4.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в подразделениях ГАПОУ СО «Ирбитский политехникум», учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- выявление демаскирующих признаков объектов ИСПДн;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, 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;
- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;
- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

4.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн ГАПОУ СО «Ирбитский политехникум» и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

4.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн);
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;
- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- эффективность применения организационных и технических мероприятий по защите информации;
- устранение ранее выявленных недостатков. Кроме того, могут проводиться необходимые измерения и расчеты, приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

4.5. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

4.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

4.7. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

4.8. По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование.

4.9. Для проведения расследования назначается комиссия с привлечением администратора безопасности. Комиссия обязана 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. После окончания расследования руководитель принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4.10. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, как правило, силами администратора безопасности и(или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

4.11. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

4.12. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в «Аттестате соответствия» (если проводилась аттестация) и(или) требованиям по безопасности персональных данных.

4.13. В ходе обследования проверяется:

- соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;
- соблюдение организационно-технических требований помещений, в которых располагается ИСПДн;
- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем положении;
- выполнение требований по защите информационных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите.

4.14. Государственный контроль состояния защиты информации осуществляется Федеральной службой по техническому и экспортному контролю России и Федеральной службой безопасности России в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

## **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 под роспись.

5.2. Пользователи должны продемонстрировать администратору безопасности и(или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор безопасности должен вести журнал учета проверок знаний и навыков пользователей.

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

5.4. Ответственным за организацию обучения и оказание методической помощи в ГАПОУ СО «Ирбитский политехникум» является администратор безопасности.

5.5. 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.

5.6. К работе в ИСПДн допускаются только сотрудники прошедшие первичный инструктаж ОБ в ИСПДн и показавшие твердые теоретические знания и практические навыки.

5.7. Администратор безопасности должен иметь профильное образование (либо дипломы о повышении квалификации) в области защиты информации. Рекомендуется прохождение администратором специализированных курсов по администрированию средств защиты информации, используемых в ИСПДн.

## **6. ПОРЯДОК ПРОВЕРКИ ЭЛЕКТРОННОГО ЖУРНАЛА ОБРАЩЕНИЙ К ИСПДН**

6.1. Настоящий раздел Положения определяет порядок проверки электронных журналов обращений к ресурсам ИСПДн.

6.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИСПДн.

6.3. Право проверки электронного журнала обращений имеют:

- администратор безопасности;
- ответственный за защиту информации;
- руководитель.

6.4. На технических средствах ИСПДн, на которых установлены специализированные средства защиты информации (далее – СЗИ) типа «Страж», «Secret Net» и другие, проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

6.5. Проверке подлежат все электронные журналы ИСПДн.

6.6. Проверка должна проводиться не реже чем один раз в неделю с целью своевременного выявления фактов нарушения требований настоящего Положения.

6.7. Факты проверок электронных журналов отражаются в специальном «Журнале учета проверок электронных журналов». После каждой проверки Администратор безопасности делает соответствующую отметку в журнале и ставит свою роспись.

## **7. ПРАВИЛА АНТИВИРУСНОЙ ЗАЩИТЫ**

7.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения (ПО), компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и



сопровождающих компьютеры в составе ИСПДн, за их выполнение. Настоящие правила распространяются на все объекты ИСПДн ГАПОУ СО «Ирбитский политехникум».

7.2. К использованию на компьютерах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

7.3. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности.

7.4. Администратор безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

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

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

7.7. 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).

7.8. Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности персональных данных определенного для данной ИСПДн класса. Настройку средств антивирусной защиты выполняет администратор безопасности.

7.9. 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.

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

7.11. На компьютеры запрещается установка программного обеспечения, не связанного с

выполнением функций, предусмотренных технологическим процессом обработки информации.

7.12. 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 безопасности) должен провести внеочередной антивирусный контроль компьютера.

7.13. 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 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.

7.13. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за защиту информации.

7.14. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

## **8. ПРАВИЛА ПАРОЛЬНОЙ ЗАЩИТЫ**

8.1. 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.

8.2. 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 администратора безопасности.

8.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ОВТ 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.

8.4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

8.5. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение руководителю структурного подразделения. Запечатанные конверты (пеналы) с паролями исполнителей должны храниться в недоступном месте у руководителя структурного подразделения.

8.6. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

8.7. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором безопасности (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания начальника отдела.

8.8. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности.

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

8.10. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

## **9. ПРАВИЛА ОБНОВЛЕНИЯ ОБЩЕСИСТЕМНОГО И ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ИСПДн, ВНЕСЕНИЯ ИЗМЕНЕНИЙ В КОНФИГУРАЦИЮ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

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

9.2. Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за эксплуатацию конкретной ИСПДн.

9.3. Право внесения изменений в конфигурацию аппаратно-программных средств, защищенных ИСПДн предоставляется:

- в отношении системных и прикладных программных средств – администратору безопасности по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн;

- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты – администратору безопасности по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн.

9.4. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников и подразделений, **запрещено**.

9.5. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн, а также средств защиты информации инициируется заявкой ответственного за эксплуатацию ИСПДн.

9.6. 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);
- изменение настроек средств защиты информации;
- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

9.7. Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

9.8. Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений. После чего заявка передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке ИСПДн.

9.9. 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 безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

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

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

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

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

9.14. Формат записей «Журнала учета нештатных ситуаций в работе информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационных систем персональных данных» устанавливается приказом руководителя Учреждения.

9.15. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации, который в свою очередь связывается с сотрудниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкциям. В данном случае администратор безопасности 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 в работе информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационных систем персональных данных» у ответственного за защиту информации.

9.16. Копии заявок могут храниться у администратора безопасности:

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

9.17. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора безопасности и сотрудника ответственного за эксплуатацию данной 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 администратором безопасности ИСПДн.

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

- руководитель;
- ответственный за защиту информации;
- администратор безопасности.

10.5. Пользователю ИСПДн категорически запрещается:

- обрабатывать конфиденциальную информацию с отключенными СЗИ;
- менять настройки СЗИ.

10.6. Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

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. Настоящее Положение устанавливает порядок охраны (сдачи под охрану) защищаемых помещений ИСПДн.

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

11.3. Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем и передаётся на пост охраны.

11.4. При отсутствии сотрудников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа, о чем составляется акт.

11.5. При закрытии помещений и сдачей их под охрану 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 убираются для хранения в опечатываемый сейф (металлический шкаф).

11.6. Помещение сдается под охрану следующим образом:

- опечатывается помещение и пенал с ключами;
- получается подтверждение от охранника о включении сигнализации и постановке помещения под охранную сигнализацию;
- факт опечатывания помещения подтверждается охранником;
- сдается помещение и опечатанный пенал с ключами, под роспись с указанием даты и времени сдачи под охрану.

11.7. Сотрудник, имеющий право на вскрытие помещений:

- получает на посту охраны пенал с ключами от помещения под роспись в Журнале с указанием даты и времени;
- проверяет целостность оттиска печати на пенале;
- производит запись в Журнале о вскрытии помещения с указанием фамилии и времени;
- производит проверку оттиска печати на двери помещения и исправность запоров;
- вскрывает помещение.

11.8. При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и(или) ответственному за защиту информации. Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.



11.9. Руководитель, ответственный за защиту информации и администратор безопасности организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

11.10. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за защиту информации, или руководителю, или администратору безопасности. Помещения вскрывать запрещается.

11.11. Помещения вскрываются ответственным за помещение, или руководителем, или ответственным за защиту информации в присутствии сотрудника охраны с составлением акта.

11.12. При передаче дежурства, если помещение в течение дня не вскрывалось, а также в выходные и праздничные дни принимающая дежурство смена поста охраны проверяет целостность печатей на дверях и пенале с ключами с отражением в «Журнале приема и сдачи дежурства» и «Журнале приема (сдачи) под охрану режимных помещений и ключей от них».

11.13. В соответствии с требованиями данного Положения при обработке защищаемой информации в ИСПДн исключить не контролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИСПДн, определенных соответствующим приказом.

## 12. ПОРЯДОК УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ

12.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

12.2. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») **запрещено**.

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

В заявке указывается:

– содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

12.4. Заявку рассматривает руководитель, визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем подписывает задание администратору безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

12.5. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 360 дней.

12.6. После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты, соответствующие требованиям безопасности, указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя – администратор безопасности.

12.7. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное (-ые) значение (-ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему.

12.8. Исполненные заявка и задание (за подписью администратора безопасности) передаются руководителю на хранение.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ИСПДн;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

### **13. ПОРЯДОК УПРАВЛЕНИЯ МАШИННЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ**

13.1. Настоящий порядок устанавливает основные требования к организации учета и использования машинных носителей данных, предназначенных для обработки и хранения персональных данных в ИСПДн.

13.2. Ответственность за организацию учета и использования машинных носителей данных, предназначенных для обработки и хранения персональных данных, возлагается на администратора безопасности.

13.3. Учет машинных носителей информации осуществляется в соответствии с формой учетной документации.

13.4. Все машинные носители данных, используемые при работе со средствами вычислительной техники (СВТ) для обработки и хранения персональных данных, должны обязательно регистрироваться и учитываться. Допускается автоматизированный учет машинных носителей информации.

13.5. Проверка наличия машинных носителей данных, предназначенных для обработки и хранения персональных данных, проводится в сроки, установленные настоящим порядком.

13.6. Вынос съемных носителей за пределы контролируемой зоны запрещен. Периодические проверки (не реже одного раза в месяц) наличия всех учтенных носителей в пределах контролируемой зоны проводятся администратором безопасности и(или) руководителем подразделения. В случае выявления факта выноса съемного носителя за пределы контролируемой зоны инициируется служебная проверка. Факт фиксируется в журнале учета нештатных ситуаций ИСПДн.

13.7. Запрещено использование в служебных целях личных, неучтенных носителей информации. Периодические проверки (не реже одного раза в месяц) использования личных, неучтенных носителей в пределах контролируемой зоны проводятся администратором безопасности и(или) руководителем подразделения. В случае выявления факта использования личных, неучтенных носителей в пределах контролируемой зоны инициируется служебная проверка. Факт фиксируется в журнале учета нештатных ситуаций ИСПДн, носитель изымается по акту для проведения процедуры принудительного стирания информации, после которой возвращается владельцу полностью отформатированным.

13.8. Учет машинных носителей информации

13.8.1. К машинным носителям информации относятся:

- магнитные ленты в кассетах;
- съемные носителя информации всех видов и способов подключения;
- несъемные жесткие магнитные диски.

13.8.2. Каждый машинный носитель данных, применяемый при обработке персональных данных в ИСПДн, должен иметь гриф – «конфиденциально».

13.8.3. Персональную ответственность за сохранность полученных машинных носителей данных и предотвращении несанкционированного доступа к записанной на них информации несет сотрудник, получивший эти носители.

13.8.4. При обработке персональных данных на СВТ должен соблюдаться следующий общий порядок учета, хранения и уничтожения машинных носителей данных.

13.8.5. Учет машинных носителей данных, предназначенных для записи персональных данных производится в «Журнале учета машинных носителей».

13.8.6. Каждому носителю информации присваивается учетный номер, который состоит из кода машинного носителя, номера объекта и порядкового номера по Журналу учета машинных носителей информации.

13.8.7. Учетный номер и гриф «конфиденциально» наносятся на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.

13.8.8. Хранение их должно осуществляться в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

13.8.9. Машинные носители данных после стирания с них персональных данных, с учета не снимаются, а хранятся наравне с другими машинными носителями.

13.8.10. В последующем эти носители используются для записи персональных данных. Если носители не пригодны для дальнейшего использования, они подлежат уничтожению по соответствующему акту.

13.8.11. О фактах утраты машинных носителей с грифом «конфиденциально» незамедлительно докладывается руководству и администратору безопасности, проводится служебное расследование.

13.8.12. Машинные носители данных должны пересылаться, по возможности, в металлических коробках, помещаемых в пакет, в упаковках, конвертах тем же порядком, что и конфиденциальные документы. На пакетах, упаковках, конвертах с носителями делается надпись: «Осторожно, машинные носители информации. Не прошивать».

13.8.13. Машинные носители данных выдаются операторам или другим лицам, участвующим в обработке информации, для работы под расписку в Журнале учета машинных

носителей информации. По завершению работы машинные носители данных сдаются ответственному руководителю подразделения за их хранение.

13.8.14. Копирование информации, содержащей персональные данные, с машинных носителей производится с разрешения руководства ГАПОУ СО «Ирбитский политехникум» по заявке руководителя отдела.

13.8.15. Машинные носители с персональными данными, утратившими практическое значение или пришедшие в негодность, уничтожаются по соответствующему акту.

13.8.16. При подготовке документов должны соблюдаться следующие особенности учета, хранения и уничтожения машинных носителей данных.

13.8.17. Машинные носители данных, предназначенные для записи персональных данных, выдаются сотрудникам по письменному разрешению руководства ГАПОУ СО «Ирбитский политехникум» в необходимом для работы количестве под расписку в Журнале учета машинных носителей информации.

13.8.18. Несъемные жесткие магнитные диски закрепляются за сотрудником, ответственным за СВТ, в котором они установлены.

13.8.19. В случае повреждения машинных носителей данных, содержащих персональные данные, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся администратору безопасности.

13.8.20. В случае необходимости (командировка, отпуск и т. д.) машинные носители с персональными данными, сдаются сотрудником ответственному лицу на постоянное или временное хранение в опечатанном виде. При этом на упаковке указывается срок их хранения, заверенный личной подписью сотрудника. По истечению указанного срока информация может быть уничтожена, а носители могут повторно использоваться.

13.8.21. Копирование персональных данных, с машинных носителей с целью передачи другим сотрудникам производится с разрешения начальника отдела.

13.8.22. Копирование осуществляется только на тех СВТ, на которых разрешена обработка персональных данных, и только на те носители, которые соответствуют грифу «конфиденциально».

13.8.23. Передача скопированной информации третьим лицам производится по письменному разрешению руководства ГАПОУ СО «Ирбитский политехникум».

13.8.24. Хранящиеся на магнитных носителях и потерявшие актуальность персональные данные должны своевременно стираться (уничтожаться). Ответственность за это несет владелец информации.

13.9. Начальник отдела не реже одного раза в год создает комиссию по проверке наличия и условий хранения персональных данных.

### 13.10. Порядок уничтожения машинных носителей, содержащих персональные данные

13.10.1. 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.

13.10.2. 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).

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

13.10.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

13.10.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

13.10.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИСПДн, ответственный за защиту информации, администратор безопасности.

## 14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

14.1. Требования настоящего Положения обязательны для всех сотрудников обрабатывающих конфиденциальную информацию (персональные данные).

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



/ Н.Н. Журавлева /

Приложение 2 к Приказу  
 ГАПОУ СО «Ирбитский политехникум»  
 от «25» декабря 2015 г. № 229

*Типовая форма журнала поземлярного учета средств защиты информации, эксплуатационной и технической документации к ним*

№ п/п	Наименование средства защиты информации, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СЗИ, эксплуатационной и технической документации к ним	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СЗИ			Отметка об изъятии СЗИ из аппаратных средств			Примечание
			От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя	Дата и расписка в получении	Ф.И.О. пользователя, производившего подключение (установку)	Дата подключения и подписи лиц, производших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14



Директор / Н.Н. Журавлева /













