Приложение № 7
к приказу генерального
директора Саморегулируемой
организации Ассоциации
«Альянс строителей
Оренбуржья»

от 01.08.2016г. № 15/1

# ПОЛОЖЕНИЕ
# по обеспечению безопасности конфиденциальной информации при ее обработке в автоматизированных системах и защищаемых помещениях Саморегулируемой организации Ассоциации «Альянс строителей Оренбуржья»

## 1. Общие положения

1.1. Данное Положение по обеспечению безопасности конфиденциальной информации при ее обработке в автоматизированных системах и защищаемых помещениях Саморегулируемой организации Ассоциации «Альянс строителей Оренбуржья» (далее – СРО) разработано с учетом специальных требований и рекомендаций по технической защите конфиденциальной информации, утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282.

1.2. Положение определяет порядок работы персонала в части обеспечения безопасности информации, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей конфиденциальной информации, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок обучения персонала практике работы в автоматизированных системах (АС), порядок проверки электронного журнала обращений к АС, 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 АС, порядок охраны и допуска посторонних лиц в защищаемые помещения.

## 2. Порядок работы персонала в части обеспечения безопасности данных при их обработке в АС

Настоящий порядок определяет действия персонала АС в части обеспечения безопасности данных при их обработке в АС.

2.1. Допуск пользователей для работы на компьютерах АС осуществляется на основании приказа, который издается руководителем, и в соответствии со списком лиц допущенных к работе в АС. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы АС, а так же средств защиты информации в АС руководителем назначается администратор АС, а с целью контроля выполнения необходимых мероприятий по обеспечению безопасности - ответственный за защиту информации.

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам АС. Полномочия пользователей к информационным ресурсам определяются в списке должностных лиц, которым необходим доступ к конфиденциальной информации, утверждаемой руководителем организации. При этом для хранения информации, содержащей конфиденциальные сведения, разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей.

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

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

2.5. Запись информации, содержащей конфиденциальные данные, может, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в журнале учета машинных носителей.

2.6. 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 АС. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах обработки конфиденциальных данных и имеющий доступ к аппаратным средствам, программному обеспечению и данным АС, несет персональную ответственность за свои действия и обязан:

1) строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

2) знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах АС;

3) хранить в тайне свой пароль (пароли). В соответствии с п.п. 8.5., 8.6. данного Положения и с установленной периодичностью менять свой пароль (пароли);

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

5) выполнять требования Положения по организации антивирусной защиты в полном объеме.

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

1) 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;

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

3) 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;

4) некорректного функционирования установленных на компьютеры технических средств защиты;

5) непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически запрещается:

1) использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

2) самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АС или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

3) осуществлять обработку конфиденциальных данных в присутствии посторонних (не допущенных к данной информации) лиц;

4) записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

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

6) оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и бумажные документы, содержащие защищаемую информацию (сведения ограниченного распространения);

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

8) размещать средства АС так, чтобы с них существовала возможность визуального считывания информации.

2.8. Администратор АС (а при его отсутствии – ответственный за защиту информации) обязан:

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

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

3) производить необходимые настройки подсистемы управления доступом установленных в АС 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 АС в информационную базу СЗИ от НСД;

– 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 АС;

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

– контролировать своевременное (не реже чем один раз в год) проведение смены паролей для доступа пользователей к компьютерам и ресурсам АС;

– обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в АС;

– 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 АС;

– 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 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 АС;

– 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;

– 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 АС 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 АС;

– контролировать соответствие документально утвержденного состава аппаратной и программной части АС реальным конфигурациям АС, вести учет изменений аппаратно-программной конфигурации;

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания АС 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 АС;

– вести журнал учета нештатных ситуаций, фактов вскрытия и опечатывания СВТ, выполнения профилактических работ, установки и модификации аппаратных и программных средств СВТ;

– поддерживать установленный порядок проведения антивирусного контроля согласно требований настоящего Положения в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

– докладывать ответственному за защиту информации, ответственному за эксплуатацию АС о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

– вести документацию на АС в соответствии с требованиями нормативных документов.

2.9. Администратор АС и ответственный за защиту информации имеют право:

1) требовать от сотрудников - пользователей АС соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в АС;

2) инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов АС;

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

4) 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 АС, допускаются только зарегистрированные в журнале учета носители.

3.3. Администратор АС обязан осуществлять периодическое резервное копирование конфиденциальной информации.

3.4. Еженедельно, по окончанию работы с конфиденциальными документами (содержащими конфиденциальные данные) на компьютере, пользователь, при отсутствии администратора АС, 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 АС. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору АС, или руководителю, или ответственному за защиту информации.

3.6. Перед резервным копированием пользователь или администратор АС 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 в соответствии с п.

7 настоящего Положения.

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:

1) вставить в компьютер зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;

2) выбрать необходимый каталог (файл) для создания резервного архива;

3) при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;

4) выполнить процедуру создания резервной копии;

5) произвести копирование на отчуждаемый носитель;

6) 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 АС в специальном хранилище.

3.13. При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором АС, ответственным за защиту информации и 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 АС 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. 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 АС в соответствии с требованиями настоящего Положения возлагается на администратора АС.

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

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

## 4. Порядок контроля защиты информации в АС. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей конфиденциальных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий

4.1. Контроль защиты информации в АС - 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:

1) проверка выполнения мероприятий по защите информации в подразделениях организации, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

2) выявление демаскирующих признаков объектов АС;

3) уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

4) проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

5) проверка выполнения требований по защите АС от

несанкционированного доступа;

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

7) проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

8) оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в АС;

9) 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 АС организации 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:

1) соответствие принятых мер по обеспечению безопасности (ОБ) данных;

2) своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ;

3) 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;

4) эффективность применения организационных и технических мероприятий по защите информации;

5) устранение ранее выявленных недостатков.

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 АС 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 конфиденциальных данных, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин

невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора АС. 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.

4.8. 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 АС и (или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

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

4.10. Обследование АС проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным требованиям по безопасности конфиденциальных данных.

4.11. В ходе обследования проверяется:

1) соответствие текущих условий функционирования обследуемого объекта АС условиям, сложившимся на момент проверки;

2) соблюдение организационно-технических требований помещений, в которых располагается АС;

3) 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;

4) соответствие выполняемых на объекте АС мероприятий по защите информации данным, изложенным в настоящем положении;

5) выполнение требований по защите информационных систем от несанкционированного доступа;

6) выполнение требований по антивирусной защите.

4.12. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов

возникновения каналов утечки информации необходимо:

1) тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы и т.д.;

2) вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;

3) проверить качество установки стеклопакетов оконных приемов;

4) провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры), при необходимости для проведения данных видов работ могут привлекаться организации, имеющие соответствующие лицензии ФСБ России.

4.13. Государственный контроль состояния защиты информации осуществляется Федеральной службы 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 по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

## 5. Порядок обучения персонала практике работы в АС в части обеспечения безопасности конфиденциальных данных

5.1. Перед началом работы в АС пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

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

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

5.4. Ответственным за организацию обучения и оказание методической помощи по работе в АС в Саморегулируемой организации Ассоциации «Альянс строителей Оренбуржья» является администратор АС.

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

5.6. К работе в АС допускаются только сотрудники прошедшие

первичный инструктаж ОБ в АС и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в журнале учёта допуска к работе в АС.

## 6. Порядок проверки электронного журнала обращений к АС

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

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

6.3. Право проверки электронного журнала обращений имеют:

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

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

6.5. Если в ходе периодических, плановых или внезапных проверок АС выявлены случай НСД к информации конфиденциального характера то вступает в силу п.п. 3.7., 3.8. данного Положения.

6.6. Проверке подлежат все электронные журналы АС.

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

6.8. Факты проверок электронных журналов отражаются в специальном журнале проверок. После каждой проверки администратор АС делает соответствующую отметку в журнале и ставит свою роспись.

## 7. Правила антивирусной защиты

7.1. Настоящие правила определяют требования к организации защиты объекта АС от разрушающего воздействия вредоносного программного обеспечения (ПО), компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе АС, за их выполнение. Настоящие правила распространяются на все объекты АС организации.

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 АС.

7.4. Администратор АС 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. 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).

Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности, определенного для данной АС класса. Настройку средств антивирусной защиты выполняет администратор АС.

7.7. 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.

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

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

7.10. 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 администратором АС) должен провести внеочередной антивирусный контроль компьютера.

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

1) приостановить обработку данных в АС;

2) немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора АС, а также смежные подразделения, использующие эти файлы в работе;

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

4) провести лечение или уничтожение зараженных файлов.

7.11. Ответственность за организацию антивирусного контроля в АС в соответствии с требованиями настоящего Положения возлагается на

ответственного за защиту информации.

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

## 8. Правила парольной защиты

8.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в АС, 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 АС и контроль действий пользователей при работе с паролями возлагается на администратора АС.

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

1) пароль должен быть не менее 9 символов;

2) в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

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

4) 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.);

5) при смене пароля новое значение должно отличаться от предыдущих;

6) пользователь не имеет права сообщать личный пароль другим лицам.

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.

8.4. 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.

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

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

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

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

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

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

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 АС.

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

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

– в отношении системных и прикладных программных средств – администратору АС по согласованию с органом по аттестации, проводившим аттестацию данной АС;

– в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты – администратору АС по согласованию с органом по аттестации, проводившим аттестацию данной АС.

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

9.5. Процедура внесения изменений в конфигурацию системных и прикладных программных средств АС инициируется заявкой ответственного за эксплуатацию АС.

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

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

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

3) 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 АС. 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 АС, 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 АС для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке АС.

9.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения АС 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 АС по согласованию с органом по аттестации, проводившим аттестацию данной АС. Работы производятся в присутствии ответственного за эксплуатацию данной АС.

9.10. Установка или обновление подсистем АС 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 АС 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 АС, выполнения профилактических работ, установки и модификации программных средств на компьютерах АС, делает отметку о выполнении (на обратной стороне заявки) и в техническом паспорте.

9.14. Формат записей журнала учета нештатных ситуаций АС, выполнения профилактических работ, установки и модификации программных средств на компьютерах АС устанавливается приказом генерального директора СРО.

9.15. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом администратору АС, который в свою очередь связывается с сотрудниками органа по аттестации и в дальнейшем действует согласно их инструкций. В данном случае администратор АС обязан предпринять необходимые меры для удаления защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с данными о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на АС и журналом учета нештатных ситуаций АС, выполнения профилактических работ, установки и модификации программных средств на компьютерах АС у ответственного за защиту информации.

9.16. Копии заявок могут храниться у администратора АС:

– для восстановления конфигурации АС после аварий;

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

– для проверки правильности установки и настройки средств защиты АС.

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

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

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

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

В заявке указывается:

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

2) должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;

3) имя пользователя (учетной записи) данного сотрудника;

4) полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в АС).

9.21. 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 АС.

9.22. В соответствии с документацией на средства защиты от несанкционированного доступа, администратор АС производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам АС 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.

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

9.24. Сотруднику, зарегистрированному в качестве нового пользователя АС, 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.

9.25. Исполненные заявка и задание (за подписью администратора АС) передаются руководителю на хранение.

Они могут впоследствии использоваться:

1) для восстановления полномочий пользователей после аварий АС;

2) для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам АС при разборе конфликтных ситуаций;

3) для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам АС.

## 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.

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 АС.

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

- генеральный директор;
- администратор безопасности информационных систем;
- администратор АС.

10.5. Пользователю АС категорически запрещается:

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

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

10.7. Если в ходе периодических, плановых или внезапных проверок АС выявлено нарушение требования п. 10.5. то вступает в силу п.п. 3.7., 3.8. данного Положения.

10.8. 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 АС.

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

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

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

11.4. 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).

11.5. Помещение сдается под охрану следующим образом:

1) опечатывается помещение и пенал с ключами;

2) получается подтверждение от охранника о включении сигнализации и постановке помещения под охранную сигнализацию;

3) факт опечатывания помещения подтверждается охранником;

4) сдается помещение и опечатанный пенал с ключами, под роспись с указанием даты и времени сдачи под охрану.

11.6. Сотрудник, имеющий право на вскрытие помещений:

1) получает на посту охраны пенал с ключами от помещения под роспись в журнале с указанием даты и времени;

2) проверяет целостность оттиска печати на пенале;

3) производит запись в журнале о вскрытии помещения с указанием фамилии и времени;

4) производит проверку оттиска печати на двери помещения и исправность запоров;

5) вскрывает помещение.

11.7. 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.

11.8. Руководитель, администратор безопасности информационных систем и администратор АС организуют проверку АС 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 охранник сообщает о случившемся ответственному за помещение, администратору безопасности информационных систем, генеральному директору и администратору АС. Помещения вскрывать запрещается.

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

Если обнаружено вторжение в защищаемое помещение, далее процедура происходит в соответствии с п. 10.8 настоящего Положения.

11.11. 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 (сдачи) под охрану режимных помещений и ключей от них.

11.12. В соответствии с требованиями данного Положения при обработке защищаемой информации в АС исключить неконтролируемое пребывание посторонних лиц в пределах границ контролируемой зоны АС, определенных 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 АС. 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 (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

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

12.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию АС, ответственный за защиту информации, администратор АС.

## 13. Заключительные положения

13.1. Требования настоящего Положения обязательны для всех сотрудников СРО, обрабатывающих конфиденциальную информацию.

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

Приложение № 1
к положению по обеспечению безопасности конфиденциальной информации при ее обработке в автоматизированных системах и защищаемых помещениях Саморегулируемой организации Ассоциации «Альянс строителей Оренбуржья»

# ТИПОВАЯ ФОРМА
## журнала поэкземплярного 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 | |
|---|---|---|---|---|---|---|
| | | | От кого получены | Дата и номер сопроводительного письма | Ф.И.О. пользователя | Дата и расписка в получении |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| Отметка о подключении (установке) СЗИ | | | Отметка об изъятии СЗИ из аппаратных средств | | | Примечание |
|---|---|---|---|---|---|---|
| Ф.И.О. пользователя, производившего подключение (установку) | Дата подключения (установки) и подписи лиц, произведших 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 | |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |

Приложение № 2
к положению по обеспечению
безопасности конфиденциальной
информации при ее обработке в
автоматизированных системах и
защищаемых помещениях
Саморегулируемой организации
Ассоциации «Альянс строителей
Оренбуржья»

# ТИПОВАЯ ФОРМА
## журнала учета машинных носителей информации

| п/п | Регистрационный (учетный) номер носителя | Вид носителя | Тип носителя и его емкость | Дата поступления |
|---|---|---|---|---|
| | 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 |
| | | | | |

\

Приложение № 3
к положению по обеспечению
безопасности конфиденциальной
информации при ее обработке в
автоматизированных системах и
защищаемых помещениях
Саморегулируемой организации
Ассоциации «Альянс строителей
Оренбуржья»

# ТИПОВАЯ ФОРМА
## журнала учета хранилищ

| п/п | Регистрационный (учетный) номер хранилища | Вид хранилища | Дата постановки на учет | Фамилия и подпись принявшего (ответственного), дата |
|---|---|---|---|---|
| | 2 | 3 | 4 | 5 |
| | | | | |

| Место расположения (номер помещения) | Дата и номер акта о выводе из эксплуатации | Примечание |
|---|---|---|
| 6 | 7 | 8 |
| | | |


Прошито, пронумеровано
двадцать пять
листа(ов)
2016г.
САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ
ДЛЯ ДОКУМЕНТОВ