МАРИЙ ЭЛ РЕСПУБЛИКЫН
ЧОНГЫМАШ,
АРХИТЕКТУР ДЕН
ИЛЕМ КОММУНАЛЬНЫЙ
ОЗАНЛЫК
МИНИСТЕРСТВЫЖЕ

МИНИСТЕРСТВО
СТРОИТЕЛЬСТВА,
АРХИТЕКТУРЫ И ЖИЛИЩНО-
КОММУНАЛЬНОГО
ХОЗЯЙСТВА
РЕСПУБЛИКИ МАРИЙ ЭЛ

П Р И К А З

от «17» июля 2009 г. № 304

Об утверждении инструкций для работы с автоматизированными системами Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», а также в целях обеспечения режима конфиденциальности проводимых работ и в соответствии с требованиями руководящих документов ФСТЭК России по защите информации, содержащей персональные данные, обрабатываемой на объектах информатизации

п р и к а з ы в а ю:

1. Утвердить Инструкцию пользователя автоматизированной системы (Приложение №1).
2. Утвердить Инструкцию по организации парольной защиты министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл (Приложение №2).
3. Утвердить Инструкцию по организации антивирусной защиты автоматизированной системы министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл (Приложение №3).

4. Утвердить Инструкцию администратора безопасности автоматизированной системы министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл (Приложение №4).

5. Ведущему специалисту-эксперту отдела формирования информационных ресурсов в градостроительстве Кузнецову А.Ю. ознакомить с инструкциями заинтересованных государственных гражданских служащих Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл.

Министр В.Н.Попов

Кузнецов А.Ю.
63-80-46

Приложение №1
к приказу Минстроя и ЖКХ
Республики Марий Эл
от « » _____ 2009 г. №

Инструкция пользователя автоматизированной системы (АС)

Общие обязанности сотрудников министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл по обеспечению информационной безопасности при работе с АС

Каждый сотрудник министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным автоматизированной системы (АС), несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции (РС);
- хранить в тайне свой пароль (пароли). В соответствии с «Инструкцией по организации парольной защиты автоматизированной системы» с установленной периодичностью менять свой пароль (пароли);
- передавать для хранения установленным порядком свое индивидуальное устройство идентификации Touch Memory, личную ключевую дискету и другие реквизиты разграничения доступа только руководителю своего подразделения или ответственному за информационную безопасность в подразделении (в пенале, опечатанном своей личной печатью);
- если сотруднику (исполнителю) предоставлено право защиты (подтверждения подлинности и авторства) документов, передаваемых по технологическим цепочкам в АС, при помощи электронной цифровой подписи, то он дополнительно обязан

соблюдать все требования «Порядка работы с ключевыми дискетами»;

- надежно хранить и никому не передавать личную печать и использовать ее только для опечатывания пенала с личной ключевой дискетой (и другими реквизитами доступа) при передаче его на хранение ответственному за информационную безопасность своего технологического участка или руководителю подразделения;
- выполнять требования «Инструкции по организации антивирусной защиты АС министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл» в части касающейся действий пользователей РС АС;
- немедленно вызывать ответственного за безопасность информации и ставить в известность руководителя отдела в случае утери персональной ключевой дискеты, индивидуального устройства идентификации Touch Memory или при подозрении компрометации личных ключей и паролей, а также при обнаружении:
  - нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах РС или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной РС;
  - несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств РС;
  - отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию РС, выхода из строя или неустойчивого функционирования узлов РС или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
  - некорректного функционирования установленных на РС технических средств защиты;
  - непредусмотренных формуляром РС отводов кабелей и подключенных устройств;
- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним РС.

Сотрудникам категорически ЗАПРЕЩАЕТСЯ:

- использовать компоненты программного и аппаратного обеспечения АС в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами рабочих станций;
- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- передавать кому-либо свою персональную ключевую дискету (кроме ответственного за информационную безопасность или руководителя своего подразделения установленным порядком), делать неучтенные копии ключевой дискеты (на любой другой носитель), снимать с дискеты защиту записи и вносить какие-либо изменения в файлы ключевой дискеты;
- использовать свою ключевую дискету для формирования цифровой подписи любых электронных документов, кроме регламентированных технологическим процессом на его рабочем месте;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свою персональную ключевую дискету, 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. Об обнаружении такого рода ошибок – ставить в известность ответственного за безопасность информации и руководителя своего подразделения.

Приложение №2
к приказу Минстроя и ЖКХ
Республики Марий Эл
от « » _____ 2009 г. №

Инструкция

по организации парольной защиты министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в локальной сети министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл далее ЛС, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ЛС и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на сотрудников отдела формирования информационных ресурсов в градостроительстве, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

2. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

   - длина пароля должна быть не менее 6 символов;
   - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
   - 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 предыдущего не менее чем в 3 позициях;
- личный пароль пользователь не имеет права сообщать никому.

3. При наличии в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие 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 ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей).

4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 90 дней.

5. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться уполномоченными сотрудниками отдела формирования информационных ресурсов в градостроительстве – администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой.

6. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.5 настоящей Инструкции.

7. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя отдела в опечатанном личной печатью пенале (возможно вместе с персональными ключевыми дискетами и идентификатором Touch Memory).

Приложение №3
к приказу Минстроя и ЖКХ
Республики Марий Эл
от « » _____ 2009 г. №

Инструкция

по организации антивирусной защиты АС министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл

1. Общие положения.

1.1. Настоящая Инструкция определяет требования к организации защиты АС министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл (далее - министерство) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих АС, за их выполнение.

1.2. Под компьютерным вирусом подразумевается программа, обязательным (необходимым) свойством которой является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Кроме того, данная программа не выполняет полезных действий или даже может приносить вред, без привлечения и информирования пользователя.

2. Антивирусные программные средства.

2.1. К использованию в министерстве допускаются только лицензионные сертифицированные антивирусные средства:

- приобретаемые самостоятельно министерством, рекомендованные к применению отделом формирования информационных ресурсов в градостроительстве.

2.2. Установка средств антивирусного контроля на рабочих станциях и серверах локальной вычислительной сети осуществляется уполномоченными сотрудниками отдела формирования информационных ресурсов в градостроительстве (далее - ответственными за антивирусный контроль). Настройка параметров средств антивирусного контроля осуществляется сотрудниками отдела формирования информационных

ресурсов в градостроительстве в соответствии с руководствами по применению конкретных антивирусных средств.

2.3. При настройке параметров антивирусных средств для проверки файлов, записанных на жестких магнитных дисках пользовательских станций, должно быть предусмотрено:

- периодичность автоматической проверки и лечения всех файлов не реже одного раза в месяц;
- возможность проверки и лечения всех файлов или по определенному шаблону (в определенных каталогах) по мере необходимости.

2.4. При настройке параметров антивирусных средств, предназначенных для проверки файлов пользовательских станций, записанных на сменных машинных носителях информации должны выполняться следующие требования:

- первое обращение к сменному носителю информации должно производиться через антивирусное ПО;
- проверки (при необходимости лечение) должны проводиться в автоматическом режиме;
- проверки должны осуществляться в минимально короткое время, без предварительной проверки загрузочных секторов и поиска вирусов в оперативной памяти.

3. Действия по предотвращению проникновения вирусов в ЛВС

3.1. Установка (изменение) системного и прикладного программного обеспечения осуществляется сотрудниками отдела формирования информационных ресурсов в градостроительстве. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено отделом формирования информационных ресурсов в градостроительстве на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка, лицом, установившим (изменившим) программное обеспечение.

3.2. Сотрудникам других отделов **запрещается** самостоятельно устанавливать, модифицировать или удалять программы и их компоненты, а также запускать программы с принесенных дискет и компакт-дисков.

3.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, программы и их компоненты), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных

носителях (магнитных и магнитооптических дисках, лентах, CD-ROM и т.п.).

3.4. Разархивирование и контроль входящей информации, поступающей по каналам электронной почты, осуществляется до передачи поступившей информации исполнителю. До проведения антивирусного контроля файлы запрещается копировать на сетевые диски отделов и в архивы электронной почты. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой.

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

3.6. Проверку на вирусы информации, поступающей на съемных машинных носителях, производит ответственный за антивирусный контроль, либо пользователь рабочей станции.

3.7. Ежедневно администратор ЛВС Управления обязан проводить проверку на наличие вирусов на всех серверах.

3.8. 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 обязан немедленно оповестить ответственного за антивирусный контроль.

4. Действия в случае обнаружения вируса

4.1. В случае обнаружения вируса на сервере ЛВС и рабочих станциях ответственный за антивирусный контроль или администратор сети обязан:

- при необходимости остановить работу ЛВС;
- сообщить начальнику отдела о факте заражения;
- провести лечение или уничтожение зараженных файлов;
- провести проверку всех рабочих станций пользователей, которые допущены к работе с данным сетевым ресурсом;
- установить владельца зараженного файла(ов);
- установить причины заражения вирусом и принять соответствующие меры по предотвращению подобных ситуаций;
- по факту обнаружения зараженных вирусом файлов составить служебную записку на имя начальника отдела формирования информационных ресурсов в градостроительстве, в которой указать предположительный источник (отправителя, владельца и т.д.) зараженного

файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

4.2. В случае обнаружения файлов, зараженных компьютерными вирусами, пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за антивирусный контроль и/или начальника отдела;
- не начинать работу до устранения причины заражения вирусом и выполнения антивирусных мероприятий;
- в случае обнаружения компьютерных вирусов на сменных машинных носителях информации клиента, вернуть носитель клиенту, без обработки, записанной на нем информации.

4.3. Отделом формирования информационных ресурсов в градостроительстве по фактам обнаружения зараженных вирусом файлов, проводится служебное расследование, в ходе которого выясняются обстоятельства заражения АС вирусами, устанавливаются виновные лица, определяется нанесенный министерству ущерб. Результаты служебного расследования докладываются руководителю министерства для принятия соответствующих мер.

5. Ответственность

5.1. Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем АС министерства, в соответствии с требованиями настоящей Инструкции возлагается на руководителя отдела формирования информационных ресурсов в градостроительстве.

5.2. Ответственность за проведение мероприятий антивирусного контроля возлагается на ответственных за обеспечение безопасности информации.

Сотрудники подразделений, являющиеся пользователями АС министерства несут ответственность за невыполнение требований п.п. 3.6, 4.2 настоящей Инструкции.

5.3. Периодический контроль за состоянием антивирусной защиты в АС министерства, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками отделов осуществляется отделом формирования информационных ресурсов в градостроительстве не реже одного раза в год.

5.4. Ответственность за антивирусный контроль в АС министерства в целом возлагается на начальника отдела формирования информационных

ресурсов в градостроительстве.

Приложение №4
к приказу Минстроя и ЖКХ
Республики Марий Эл
от « » _____ 2009 г. №

Инструкция

администратора безопасности автоматизированной системы министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл

1. Общие положения

1.1. Настоящая инструкция разработана на основании «Концепции информационной безопасности», «Положения о системе защиты информации», «Положения о порядке организации и проведения работ по защите», «Положения о разрешительной системе допуска исполнителей к документам и сведениям».

1.2. Инструкция определяет основные задачи, функции, обязанности, права и ответственность Администратора безопасности автоматизированной системы (далее – АС).

1.3 Администратор безопасности АС (далее – Администратор) назначается из состава отдела формирования информационных ресурсов в градостроительстве и является лицом, выполняющим функции по ОБИ, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники АС, в пределах своей зоны ответственности (функции Администратора могут быть распределены между несколькими сотрудниками решением начальника отдела).

1.4. Закрепление функциональных обязанностей и разделение зон ответственности производится приказом руководителя.

1.5. В своей деятельности Администратор руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты информации и обеспечивает их выполнение администраторами ЛВС, баз данных и пользователями АС.

1.6 Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

2. *Задачи и функции Администратора*

2.1 Основными задачами Администратора являются:

- сопровождение средств защиты информации от несанкционированного доступа (далее – СрЗИ от НСД) и основных технических средств и систем (далее – ОТСС);
- организация разграничения доступа;
- контроль эффективности защиты информации.

2.2. Для выполнения поставленных задач на Администратора возлагаются следующие функции:

2.2.1. Допуск пользователей (разработчиков, эксплуатационного персонала) к техническим, программным средствам и информационным ресурсам.

2.2.2. Участие на стадии проектирования (внедрения) АС в разработке технологии обработки информации ограниченного доступа (далее – информации) по вопросам:

- организации порядка учета, хранения и обращения с документами и носителями информации;
- определения степени секретности отдельных документов, носителей и массивов информации;
- подготовки инструкций, определяющих задачи, функции, ответственность, права и обязанности администраторов и пользователей АС по вопросам защиты информации, а также ответственных по защите информации в процессе автоматизированной обработки информации.

2.2.3. Сопровождение СрЗИ от НСД к ней, в том числе средств криптографической защиты информации, на стадии эксплуатации АС, включая ведение служебной информации СрЗИ от НСД (управление ключевой системой, сопровождение правил разграничения доступа), оперативный контроль за функционированием СрЗИ от НСД.

2.2.4. Контроль выполнения требований действующих нормативных документов по вопросам защиты информации при обработке информации в АС.

2.2.5. Контроль соответствия общесистемной программной среды эталону (контроль целостности программного обеспечения) и проверка включаемых в АС новых программных средств.

2.2.6. Оперативный контроль за ходом технологического процесса обработки информации.

2.2.7. Методическое руководство работой администраторов и пользователей АС в вопросах обеспечения информационной безопасности.

3. Обязанности Администратора

3.1. Для реализации поставленных задач и возложенных функций Администратор ОБЯЗАН:

3.1.1. Сопровождать СрЗИ от НСД и ОТСС:

3.1.1.1. Вести учет (по вопросам ОБИ) и знать перечень установленных в подразделениях ОТСС, СрЗИ от НСД и перечень задач, решаемых с их использованием.

3.1.1.2. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на рабочих станциях (далее – РС) специальных программных и программно-аппаратных СрЗИ от НСД.

3.1.1.3. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных РС и серверов, осуществлять проверку работоспособности системы защиты после установки (обновления) программных средств АС.

3.1.1.4. Периодически проверять состояние используемых СЗИ от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

3.1.1.5. Контролировать соответствие технического паспорта объекта вычислительной техники (далее – СВТ) фактическому составу (комплектности) СВТ АС и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения в АС).

3.1.1.6. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных РС.

3.1.1.7. Вести журнал учета нештатных ситуаций, фактов вскрытия и опечатывания СВТ, выполнения профилактических работ, установки и модификации аппаратных и программных средств АС.

3.1.1.8. Проводить периодический инструктаж сотрудников подразделения (пользователей средств вычислительной техники) по правилам

работы с используемыми средствами и системами зашиты информации.

3.1.2. Организовывать разграничения доступа:

3.1.2.1. Участвовать в разработке и знать перечень защищаемых информационных ресурсов.

3.1.2.2. Разрабатывать совместно с администраторами АС решения по:

- составу доменов сети, системы доверительных отношений между ними;
- составу групп (локальных и глобальных) каждого домена;
- приписке пользователей с одинаковыми правами, статусом безопасности и характером решаемых задач к соответствующим группам;
- определению информационных связей между сегментами сети и требований к изоляции сегментов с использованием средств аппаратной безопасности сегментов;
- определению списка устройств, логических дисков, каталогов общего пользования на серверах с указанием состава допущенных к ним пользователей и режимов допуска;
- осуществлению контроля за наличием активных компьютеров сети, состоянием активных пользователей, использованием разделяемых ресурсов, процессом печати на общих принтерах;
- разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, проектированию системы почтовых ящиков, использованию СЗИ при передаче закрытых документов);
- разработке порядка выхода пользователей в сети связи общего пользования (далее – Сети) и использованию встроенных СрЗИ от НСД в сервисных программах;
- определению режимов использования СрЗИ от НСД: защита паролей, защита в протоколах передачи данных, кодирование файлов, подтверждение подлинности электронных документов (электронная цифровая подпись), подключение дополнительных алгоритмов криптографической защиты;

- разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита.

3.1.2.3. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных РС АС.

3.1.2.4. Контролировать и требовать соблюдения установленных правил по организации парольной защиты в АС.

3.1.2.5. Осуществлять оперативный контроль за работой пользователей защищенных РС, анализировать содержимое журналов событий операционных систем (далее - ОС), систем управления базами данных (далее - СУБД), пакетов прикладных программ (далее - ППП) и СЗИ от НСД всех РС и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование журналов событий РС и надлежащий режим хранения данных архивов.

3.1.2.6. Принимать участие в работах по внесению изменений в аппаратно-программную конфигурацию серверов и РС АС.

3.1.2.7. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания РС и отправке их в ремонт (контролировать стирание информации на магнитных носителях).

3.1.2.8. Организовывать учет, хранение, прием и выдачу персональных идентификаторов и ключевых дискет ответственным исполнителям, осуществлять контроль за правильностью их использования.

3.1.2.9. Осуществлять периодический контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных.

3.1.2.10. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СрЗИ от НСД, установленных на РС АС.

3.1.2.11. Требовать от пользователей стирания остаточной информации на несъёмных носителях (жестких дисках) установленным порядком, а в оперативной памяти по окончании обработки информации путем перезагрузки РС.

3.1.2.12. Контролировать обеспечение защиты конфиденциальной информации при взаимодействии абонентов с информационными сетями связи общего пользования.

3.1.3. Контролировать эффективность защиты информации:

3.1.3.1. Проводить работу по выявлению возможности вмешательства в процесс функционирования АС и осуществления НСД к информации и техническим средствам РС.

3.1.3.2. Докладывать начальнику отдела о выявленных угрозах безопасности информации, обрабатываемой в АС, об имевших место попытках НСД к информации и техническим средствам РС.

3.1.3.3. Проводить занятия с администраторами и пользователями АС по правилам работы на РС, оснащенных СрЗИ НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков, выявленных при контроле эффективности защиты информации.

3.1.3.4. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в АС.

3.2. Администратору ЗАПРЕЩАЕТСЯ:

3.2.1. Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации;

3.2.2. Использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий;

3.2.3. Самостоятельно (без согласования с подразделением автоматизации) вносить изменения в настройки серверной части АС;

3.2.4. Использовать в своих и в чьих-либо личных интересах ресурсы АС, предоставлять такую возможность другим;

3.2.5. Выключать СрЗИ от НСД без санкции руководства;

3.2.6. Передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки;

3.2.7. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы АС, блокированию доступа, потере

информации без санкции руководства и предупреждения пользователей;

3.2.8. Нарушать правила эксплуатации оборудования АС;

3.2.9. Корректировать, удалять, подменять журналы аудита.

4. Права и ответственность Администратора

4.1. Администратор имеет право:

4.1.1. Получать доступ к программным и аппаратным средствам АС, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах АС и РС пользователей.

4.1.2. Требовать от администраторов и пользователей АС выполнения инструкций по обеспечению безопасности и защите информации в АС.

4.1.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов АС.

4.1.4. Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим докладом начальнику отдела ОБИ.

4.1.5. Производить анализ защищенности АС путем применения специального программного обеспечения, осуществления попыток взлома системы защиты АС. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным уведомлением сотрудников подразделений автоматизации и ОБИ.

4.1.6. Вносить свои предложения по совершенствованию мер защиты в АС.

4.2. Администратор несет ответственность за:

4.2.1. Реализацию принятой политики информационной безопасности;

4.2.2. Программно - технические и криптографические средства защиты информации, средства вычислительной техники, информационно -

вычислительные комплексы, сети и АС обработки информации, закрепленные за ним приказом руководителя, а также за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

4.2.3. Разглашение сведений, составляющих (служебную, банковскую, коммерческую) тайну, и сведений ограниченного распространения, ставших известными ему по роду работы;

4.2.4. Качество и последствия проводимых им работ по контролю действий пользователей при работе в АС.