Проект инструкции

администратора безопасности информационных систем персональных данных (наименование оператора)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий документ определяет основные обязанности, права и ответственность администратора безопасности ИСПДн (наименование оператора).
2. Администратор безопасности назначается руководителем опера­тора или начальником подразделения, ответственного за обеспечение безопасности ПДн.
3. Администратор безопасности в своей работе руководствуется настоящей инструкцией и (указываются действующие внутренние органи­зационно-распорядительные документы, регламентирующие обработку ПДн у оператора).
4. Администратор безопасности является ответственным должно­стным лицом, уполномоченным на проведение работ по поддержанию дос­тигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.
5. Администратор безопасности осуществляет методическое руко­водство операторов, системных администраторов и других лиц, допущен­ных к работе в ИСПДн, в вопросах обеспечения защиты ПДн.
6. Требования администратора безопасности, связанные с выпол­нением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.
7. Администратор безопасности несет персональную ответствен­ность за качество проводимых им работ по контролю действий пользова­телей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ АДМИНИСТРАТОРА

БЕЗОПАСНОСТИ

2.1. Администратор безопасности обязан:

1. Знать перечень и состав ИСПДн, перечень задач, решаемых их использованием.
2. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряже­ний, регламентирующих порядок действий по обеспечению защиты ПДн.
3. Осуществлять установку, настройку и сопровождение СЗИ.
4. Осуществлять учет применяемых СЗИ, эксплуатационной и технической документации к ним.
5. Участвовать в контрольных и тестовых испытаниях и провер­ках элементов ИСПДн.
6. Участвовать в приемке новых программных средств.
7. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно Разрешительной системы доступа к информационным ресурсам, программным и техническим средствам ИСПДн.
8. Уточнять в установленном порядке обязанности пользовате­лей ИСПДн.
9. Проводить резервирование ПДн.
10. Вести учет носителей ПДн.
11. Выдавать пользователям личные пароли доступа к средст­вам ИСПДн.
12. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.
13. Контролировать неизменность состояния СЗИ их параметров и режимов защиты.
14. Контролировать физическую сохранность средств и оборудо­вания ИСПДн.
15. Контролировать исполнение пользователями ИСПДн введен­ного режима безопасности, а так же правильность работы с элементами ИСПДн и СЗИ.
16. Контролировать исполнение пользователями парольной защиты.
17. Контролировать работу пользователей в сетях общего пользо­вания и международного обмена.
18. Своевременно анализировать журналы учета событий, с це­лью выявления возможных нарушений.
19. Не допускать установку, использование, хранение и размно­жение в ИСПДн программных средств, не связанных с выполнением функциональных задач.
20. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн.
21. Оказывать помощь пользователям ИСПДн в части примене­ния СЗИ и консультировать по вопросам введенного режима защиты.
22. Периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущен­ных пользователями нарушениях установленных требований по защите информации.
23. В случае отказа работоспособности СЗИ ИСПДн принимать меры по их своевременному восстановлению и выявлению причин, при­ведших к отказу работоспособности.
24. Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, участвовать в расследовании причин их возникновения.

3. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

1. Личные пароли доступа к средствам ИСПДн выдаются пользова­телям администратором безопасности, ответственным за обеспечение безопасности ПДн или другим уполномоченным лицом.
2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
3. Правила формирования пароля:
* пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
* пароль должен состоять не менее чем из 8 символов;
* в пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (на­пример, !, $, #, %);

* запрещается использовать в качестве пароля имя входа в сис­тему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, номера ав­томобилей, телефонов и другие пароли, которые можно угадать, основыва­ясь на информации о пользователе;
* запрещается выбирать пароли, которые уже использовались ранее.

4. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

4.1. Администратор безопасности имеет право:

1. Отключать любые элементы СЗПДн при изменении конфигу­рации, регламентном техническом обслуживании или устранении неис­правностей в установленном порядке.
2. В установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн.
3. Требовать от сотрудников соблюдения правил работы в ИСПДн, приведенных в должностных инструкциях.
4. Требовать от пользователей безусловного соблюдения уста­новленной технологии обработки ПДн и выполнения требований локаль­ных документов, регламентирующих вопросы обеспечения защиты ПДн.
5. Требовать прекращения обработки информации в случае на­рушения установленной технологии обработки ПДн или нарушения функ­ционирования СЗИ.
6. Вносить свои предложения по совершенствованию СЗПДн.
7. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты ПДн в ИСПДн.

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

5.1. Администратор безопасности несет ответственность:

1. За ненадлежащее исполнение или неисполнение своих должно­стных обязанностей, предусмотренных настоящей инструкцией, другими локальными организационно-распорядительными документами, в соответ­ствии с действующим трудовым законодательством Российской Федерации.
2. За правонарушения, совершенные в процессе своей деятельно­сти в пределах, определенных действующим административным, уголов­ным и гражданским законодательством Российской Федерации.
3. За разглашение сведений конфиденциального характера и дру­гой защищаемой информации в пределах, определенных действующим ад­министративным, уголовным и гражданским законодательством Россий­ской Федерации.
4. На администратора безопасности возлагается персональная от­ветственность за работоспособность и надлежащее функционирование СЗИ ИСПДН.