

Принято:
Общим собранием
Протокол №1
от «30» августа 2018

Согласованно с учетом мнения профсоюзной
организации ГБДОУ
С.Ф. председатель ПК Сапунова С.Ф.
от «30» августа 2018

Утверждено:
Приказом №-33-от «30» августа 2018г
Заведующий ГБДОУ №53

/А.Г.Шумай/



Инструкция № 65
администратора по обеспечению безопасности информационных
систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора безопасности ИСПДн

1.2. Администратор безопасности назначается руководителем оператора или начальником подразделения, ответственного за обеспечение безопасности ПДн.

Администратор безопасности в своей работе руководствуется настоящей инструкцией и *(указываются действующие внутренние организационно-распорядительные документы, регламентирующие обработку ПДн у оператора)*.

1.3. 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.

1.4. Администратор безопасности осуществляет методическое руководство операторов, системных администраторов и других лиц, допущенных к работе в ИСПДн, в вопросах обеспечения защиты ПДн.

1.5. Требования администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.6. 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:

2.2.1. Знать перечень и состав ИСПДн, перечень задач, решаемых их использованием.

2.2.2. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий защиты ПДн.

2.2.3. Осуществлять установку, настройку и сопровождение СЗИ.

2.2.4. Осуществлять учет применяемых СЗИ, эксплуатационной и технической документации к ним.

2.2.5. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.2.6. Участвовать в приемке новых программных средств.

2.2.7. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно Разрешительной системы доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

2.2.8. Уточнять в установленном порядке обязанности пользователей ИСПДн.

2.2.9. Проводить резервирование ПДн.

2.2.10. Вести учет носителей ПДн.

2.2.11. Выдавать пользователям личные пароли доступа к средствам ИСПДн.

2.2.12. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.2.13. Контролировать неизменность состояния СЗИ их параметров и режимов защиты.

2.2.14. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.2.15. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и СЗИ.

2.2.16. Контролировать исполнение пользователями парольной защиты.

2.2.17. Контролировать работу пользователей в сетях общего пользования и международного обмена.

2.2.18. Своевременно анализировать журналы учета событий, с целью выявления возможных нарушений.

2.2.19. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.2.20. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн.

- 2.2.21.Оказывать помощь пользователям ИСПДн в части применения СЗИ и консультировать по вопросам введенного режима защиты.
- 2.2.22.Периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.
- 2.2.23.В случае отказа работоспособности СЗИ ИСПДн принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
- 2.2.24.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

- 3.1.Личные пароли доступа к средствам ИСПДн выдаются пользователям администратором безопасности, ответственным за обеспечение безопасности ПДн или другим уполномоченным лицом.
- 3.2.Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
- 3.3.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 А до Z;
 - б) строчные буквы английского алфавита от а 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 также 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:
- 4.1.2.Отключать любые элементы СЗПДн при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке.
- 4.1.3.В установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн.
- 4.1.4.Требовать от сотрудников соблюдения правил работы в ИСПДн, приведенных в должностных инструкциях.
- 4.1.5.Требовать от пользователей безусловного соблюдения установленной технологии обработки ПДн и выполнения требований локальных документов, регламентирующих вопросы обеспечения защиты ПДн.
- 4.1.6.Требовать прекращения обработки информации в случае нарушения установленной технологии обработки ПДн или нарушения функционирования СЗИ.
- 4.1.7.Вносить свои предложения по совершенствованию СЗПДн.
- 4.1.8.Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты ПДн в ИСПДн.

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

- 5.1.Администратор безопасности несет ответственность:
- 5.1.1.За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими локальными организационно-распорядительными документами, в соответствии с действующим трудовым законодательством Российской Федерации.

5.1.2. За правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5.1.3. За разглашение сведений конфиденциального характера и другой защищаемой информации в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5.1.4. На администратора безопасности возлагается персональная ответственность за работоспособность и надлежащее функционирование СЗИ ИСПДН.