ИНСТРУКЦИЯ
администратора безопасности информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет обязанности должностного лица, ответственного за обеспечение безопасности информации (в том числе персональных данных (ПДн), обрабатываемой в информационных системах ПДн (ИСПДн),далее - (администратора безопасности).

1.2. Администратор безопасности назначается приказом руководителя .

1.3. Администратор безопасности отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе ПДн, при их обработке в ИСПДн

1.4. Администратор безопасности осуществляет методическое руководство деятельностью пользователей ИСПДн в вопросах обеспечения безопасности информации.

1.5. Требования администратора безопасности, связанные с выполнением им своих 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 информации, обрабатываемой в ИСПДн .

2. ЗАДАЧИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

2.1. Основными задачами администратора безопасности являются:

- поддержание необходимого уровня защиты ИСПДн от несанкционированного доступа (НСД) к информации;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации;
- установка средств защиты информации и контроль выполнения правил их эксплуатации;
- сопровождение средств защиты информации (СЗИ) от НСД и основных технических средств и систем (ОТСС) ИСПДн ;
- периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов ИБ;
- оперативное реагирование на нарушения требований по ИБ в ИСПДн и участие в их прекращении.

2.2. В рамках выполнения основных задач администратор безопасности осуществляет:

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;
- текущий контроль технологического процесса автоматизированной обработки ПДн;

- участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности ПДн;

- контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации ;

- методическую помощь всем работникам по вопросам обеспечения безопасности ПДн.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Администратор безопасности обязан:

3.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИСПДн.

3.2. Участвовать в установке, настройке и сопровождении программных средств защиты информации.

3.3. Участвовать в приемке новых программных средств обработки информации.

3.4. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

3.5. Уточнять в установленном порядке обязанности пользователей ИСПДн при обработке ПДн.

3.6. Вести контроль осуществления резервного копирования информации.

3.7. Анализировать состояние защиты ИСПДн .

3.8. Контролировать правильность функционирования средств защиты информации и неизменность их настроек.

3.9. Контролировать физическую сохранность технических средств обработки информации.

3.10. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты информации.

3.11. Контролировать исполнение пользователями правил парольной политики.

3.12. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

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

3.14. Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) ИСПДн .

3.15. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

3.16. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.17. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.18. В случае выявления нарушений режима безопасности информации (ПДн), а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

3.19. Принимать участие в проведении работ по оценке соответствия ИСПДн _____ требованиям безопасности информации <1>.

<1> Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных", Постановление Правительства Российской Федерации от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", нормативно-правовые акты и методические документы ФСТЭК России и ФСБ России по защите персональных данных при их обработке в информационных системах персональных данных.

4. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности имеет право:

4.1. Отключать от ресурсов ИСПДн работников, осуществивших НСД к защищаемым ресурсам ИСПДн или нарушивших другие требования по ИБ.

4.2. Давать работникам обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИСПДн .

4.4. Организовывать и участвовать в любых проверках по использованию пользователями и территориальных органов телекоммуникационных ресурсов.

4.5. Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.6. Осуществлять взаимодействие с руководством и персоналом вопросам обеспечения ИБ.

4.7. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

4.8. Запрашивать и получать от Руководителей и специалистов структурных подразделений информацию и материалы, необходимые для организации своей работы.

4.9. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ ПДн.

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности несет ответственность <2>:

<2> Виновные в нарушении режима защиты ПДн, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

5.1. За организацию защиты информационных ресурсов и технических средств ИСПДн.

5.2. За качество проводимых работ по контролю действий пользователей и администраторов ИСПДн, состояние и поддержание необходимого уровня защиты информационных и технических ресурсов ИСПДн .

5.3. За разглашение сведений ограниченного доступа (коммерческая тайна, персональные данные и иная защищаемая информация), ставших известными ему по роду работы.