**АДМИНИСТРАЦИЯ МИТРОФАНОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**КАНТЕМИРОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**ВОРОНЕЖСКОЙ ОБЛАСТИ**

**Р А С П О Р Я Ж Е Н И Е**

от 03.07.2018 № 72

 с.Митрофановка

**Об утверждении Инструкции**

**администратора безопасности**

**информации информационных систем администрации Митрофановского сельского поселения Кантемировского муниципального района**

В соответствии с Федеральным законом от 06.10.2003 № 131 - ФЗ «Об общих принципах организации местного самоуправления в Российской Фе­дерации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Уставом Митрофановского сельского поселения Кантемировского муници­пального района:

 1. Утвердить Инструкцию администратора безопасности информации информационных систем администрации Митрофановского сельского поселения Кантемировского муниципального района согласно приложению.

 2. Контроль за исполнением настоящего распоряжения оставляю за собой

Глава Митрофановского

сельского поселения В.Д.Приколотин

Приложение

к распоряжению администрации

Митрофановского сельского поселения

от «03» июля 2018 года № 72

Инструкция

**администратора безопасности информации информационных систем администрации** **Митрофановского сельского поселения** **Кантемировского муниципального района**

1. **Общие положения**
	1. Настоящая инструкция определяет права и обязанности должностного лица, ответственного за обеспечение безопасности информации ограниченного доступа – ОИД (в том числе персональных данных (ПДн)), обрабатываемой в информационных системах персональных данных (ИСПДн), далее – администратора безопасности информации (администратора безопасности).
	2. Администратор безопасности информации ИСПДН назначается распоряжением администрации Митрофановского сельского поселения Кантемировского муниципального района и отвечает за обеспечение безопасности ИОД при ее обработке в ИСПДН.
	3. Администратор безопасности по вопросам обеспечения безопасности информации подчиняется ответственному за обеспечение безопасности информации в ИСПДН.
	4. Администратор безопасности информации отвечает за поддержание установленного класса защищенности информации, содержащейся в ИСПДН.
	5. Администратор безопасности информации осуществляет методическое руководство деятельности пользователей ИСПДН.
	6. Требования администратора безопасности информации, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДН.
	7. Администратор безопасности информации 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.
	8. Администратор безопасности информации обеспечивает нормальное функционирование защитных механизмов ИСПДН.
	9. Настоящая инструкция не исключает обязательного выполнения требований других действующих нормативных документов по вопросам обеспечения защиты ИОД.
2. **Задачи администратора безопасности информации**
	1. Основными задачами администратора безопасности информации являются:

- поддержание необходимого уровня защиты ИСПДН от несанкционированного доступа (НСД) к информации;

- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации (ИОД);

- установка средств защиты информации и контроль выполнения правил их эксплуатации;

- сопровождение средств защиты информации (СЗИ) и основных технических средств и систем (ОТСС) ИСПДН;

- периодическое обновление СЗИ ИСПДН;

- оперативное реагирование на нарушения требований по информационной безопасности (ИБ) в ИСПДН и участие в их прекращении.

2.2. В рамках выполнения основных задач администратор безопасности информации осуществляет:

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;

- текущий контроль технологического процесса автоматизированной обработки ИОД;

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

- управление полномочиями пользователей ИСПДН и поддержание правил разграничения доступа в ИСПДН;

- управление СЗИ в ИСПДН, в том числе параметрами настройки программного обеспечения (ПО), включая ПО СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;

- установка обновлений ПО, включая ПО СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;

- централизованное управление системой защиты информации ИСПДН;

- регистрация и анализ событий в ИСПДН, связанных с защитой информации (далее – события безопасности);

- информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИСПДН и отдельных СЗИ, а также их обучение;

- сопровождение функционирования системы защиты информации ИСПДН в ходе ее эксплуатации;

- поддержание конфигурации ИСПДН и системы защиты информации (структуры системы защиты информации, состава, мест установки и параметров настройки СЗИ, ПО и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИСПДН и системы защиты информации);

- управление изменениями базовой конфигурации ИСПДН и системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИСПДН и системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИСПДН и системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИСПДН и системы защиты информации, сохранение данных об изменениях базовой конфигурации ИСПДН и системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИСПДН и системы защиты информации;

- анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПДН и системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДН;

- определение параметров настройки ПО, включая ПО СЗИ, состава и конфигурации технических средств и ПО до внесения изменений в базовую конфигурацию ИСПДН и системы защиты информации;

- методическую помощь всем пользователям ИСПДН по вопросам обеспечения безопасности ИОД.

1. **Администратор безопасности информации имеет право:**

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

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

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

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

3.5. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное ПО и аппаратное обеспечение.

3.6. Вырабатывать предложения по дальнейшему усовершенствованию принятой политики безопасности, выбору используемого в ИСПДН ПО и аппаратного обеспечения.

1. **Администратор безопасности информации обязан:**

4.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты ИОД, обрабатываемой в ИСПДН.

4.2. Управлять конфигурацией системы защиты информации ИСПДН.

4.2.1. Разграничивать права доступа в ИСПДН.

4.2.2. Осуществлять управление изменениями конфигурации ИСПДН и системы защиты информации ИСПДН.

4.2.3. Проводить анализ потенциального воздействия планируемых изменений в конфигурации ИСПДН и системе защиты информации ИСПДН.

 4.2.4. Осуществлять документирование информации (данных) об изменениях конфигурации ИСПДН и системы защиты информации ИСПДН.

4.2.5. Осуществлять контроль безотказного функционирования технических средств, обнаружение и локализацию отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

4.2.6. Выполнять периодическое резервное копирование информации ИСПДН на резервные машинные носители информации.

4.2.7. Участвовать в установке, настройке и сопровождении программных СЗИ.

4.2.8. Участвовать в приемке новых программных средств обработки информации.

4.3. Осуществлять периодический мониторинг (контроль) защищенности ИР.

4.3.2. Осуществлять обнаружение, идентифицировать и регистрировать инциденты (события безопасности).

4.3.3. Своевременное информировать лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПДН.

4.3.4. Осуществлять мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

4.3.5. Выявлять, анализировать уязвимости системы защиты информации ИСПДН и оперативно устранять вновь выявленные уязвимости.

4.3.6. Осуществлять контроль установки обновлений ПО, включая обновления ПО СЗИ.

4.3.7. Обеспечивать контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ.

4.3.8. Осуществлять контроль состава технических средств, ПО и СЗИ.

4.3.9. Осуществлять контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей.

4.3.10. Осуществлять контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов, в том числе по передачи информации.

4.3.11. Осуществлять контроль за выполнением мер по защите технических средств.

4.3.12. Осуществлять анализ событий во время загрузки ОС.

4.3.13. Осуществлять отслеживание попыток использования ИР вне установленного рабочего времени.

4.3.14. Отслеживать изменений в перечне пользователей, допущенных к защищенным ИР.

4.3.15. Осуществлять обнаружение использования ПО, не внесенного в регламент.

4.3.16. Осуществлять обнаружение новых (неизвестных) устройств.

4.3.17. Осуществлять проверку соответствия общесистемной программной среды эталону (контроль целостности ПО).

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

4.5. Установленным порядком хранить резервные копии, регистрации фактов нарушения установленного порядка работ и попыток НСД, пароли администратора безопасности информации и пользователей пользователям ИСПДН.

4.6. Вести журнал создания резервных копий информации и необходимого программного обеспечения.

* 1. Вести журнал фактов нарушения установленного порядка работ и попыток НСД с отражением:
		1. Даты и времени начала и конца несанкционированных действий пользователя и его идентификатора.
		2. Состава несанкционированных действий.
		3. Реакции защитных механизмов ИСПДН на эти действия.

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

4.9. Контролировать исполнение пользователями правил парольной политики.

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

4.11. Оказывать помощь пользователям ИСПДН в части применения СЗИ и консультировать по вопросам введенного режима защиты.

4.12. В случае отказа работоспособности технических средств и ПО ИСПДН, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

4.13. В случае выявления нарушений режима безопасности ИОД (в том числе ПДн), а также возникновения внештатных и аварийных ситуаций, немедленно докладывать об этом ответственному по обеспечению безопасности информации и принимать необходимые меры с целью ликвидации их последствий.

* 1. В случае болезни, отпуска, командировки и в других случаях отсутствия администратор безопасности информации передает свои обязанности замещающему его лицу, назначаемому распоряжением администрации Кантемировского муниципального района.
1. **Ответственность администратора безопасности информации**

Администратор безопасности информации несет ответственность:

5.1. За качество выполнения обязанностей, установленных данной Инструкцией.

5.2. За качество проводимых работ по контролю действий пользователей, состояние и поддержание необходимого класса защищенности информации, содержащейся в ИСПДН.

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

1. **Действия администратора безопасности информации при обнаружении попыток НСД**

6.1. К попыткам НСД относятся:

- сеансы работы с ИР ИСПДН незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;

- действия третьего лица, пытающегося получить доступ (или получившего доступ) к ИР ИСПДН с использованием учетной записи администратора или другого пользователя ИСПДН, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и другие случаи ) без ведома владельца учетной записи.

6.2. При выявлении факта/попытки НСД администратор безопасности информации обязан:

- прекратить доступ к ИР со стороны выявленного участка НСД;

- доложить ответственному за обеспечение безопасности информации ИСПДН о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

- проанализировать характер НСД;

- по решению ответственного за обеспечение безопасности информации осуществить действия по выяснению причин, приведших к НСД;

- предпринять меры по предотвращению подобных инцидентов в дальнейшем.

**Лист ознакомления**