|  |  |  |
| --- | --- | --- |
| **УТВЕРЖДАЮ**Директор ОГБУ «Агентство по развитию сельских территорий Ульяновской области» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **М.А. Шпак**«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 годам.п. |  | **УТВЕРЖДАЮ**Заместитель Министра сельского, лесного хозяйства и природных ресурсов Ульяновской области \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **А.И. Братяков**«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 года м.п. |

**ИНСТРУКЦИЯ**

**администратора безопасности информационных систем**

**персональных данных в Министерстве сельского, лесного хозяйства и природных ресурсов Ульяновской области и ОГБУ «Агентство по развитию сельских территорий Ульяновской области»**

**I. Общие положения**

Настоящая Инструкция определяет функции, права и обязанности Администратора безопасности по вопросам обеспечения информационной безопасности конфиденциальной информации, в т. ч. персональных данных при работе в ИСПДн Министерства сельского, лесного хозяйства и природных ресурсов Ульяновской области и ОГБУ «Агентство по развитию сельских территорий Ульяновской области» (далее – Учреждения).

Администратор безопасности назначается из числа сотрудников Учреждения и обеспечивает правильность использования и нормальное функционирование установленной системы защиты информации (СЗИ).

**II. Основные функции Администратора безопасности информации.**

2.1. Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности и защиты персональных данных при проведении работ в ИСПДн Учреждения.

2.2. Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в ИСПДн:

* реализация полномочий доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру, сетевым ресурсам и т.д.);
* ввод описаний пользователей ИСПДн в информационную базу СЗИ от несанкционированного доступа (НСД).
* своевременное удаление описаний пользователей из базы данных СЗИ при изменении списка допущенных к работе в ИСПДн лиц.

2.3. Контроль за периодическим проведением смены паролей для доступа к ИСПДн пользователями.

2.4. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн:

* введение в базу данных СЗИ от НСД, внедренной в ИСПДн, описания событий, подлежащих регистрации в системном журнале;
* регулярное проведение анализа системного журнала для выявления попыток НСД к защищаемым ресурсам;
* своевременное информирование руководителя, ответственного за эксплуатацию ИСПДн Учреждения о несанкционированных действиях персонала и проведение расследования попыток НСД.

2.6 Сопровождение антивирусной подсистемы и системы защиты от программно-математических воздействий:

* поддержание установленного порядка и правил антивирусной защиты информации в ИСПДн от компьютерных вирусов;
* периодическое обновление антивирусных средств (баз данных), внедрённых в ИСПДн, контроль за соблюдением пользователями порядка и правил проведения антивирусного тестирования ИСПДн Учреждения;

2.7 Сопровождение , подсистемы межсетевого экранирования::

* анализ журнала межсетевого экрана на предмет выявления запрещенных взаимодействий.

**III. Обязанности Администратора безопасности:**

3.1. Администратор безопасности обязан:

* обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;
* проводить инструктаж пользователей по правилам работы в ИСПДн с внедренными средствами защиты;
* докладывать руководителю, ответственному за эксплуатацию ИСПДн Учреждения о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;
* следить за выполнением пользователями своих обязанностей, в т. ч. за проведением периодических антивирусных проверок;
* по всем вопросам, касающимся функционирования средств защиты информации и неотраженным в настоящей инструкции, обращаться к руководствам конкретных средств защиты, имеющимся на установочных дисках этих средств.

**IV. Права Администратора безопасности:**

4.1. Администратор безопасности имеет право:

* участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
* требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
* проходить повышение своей квалификации на учебных курсах, в том числе на курсах по средствам защиты, установленным в локальной сети Учреждения.