

Приложение 4
к Политике аудита
информационной безопасности
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

ПЛАН
проведения периодического внутреннего аналитического аудита
информационной безопасности

(наименование структурного подразделения)

Администрация муниципального образования Северский муниципальный район Краснодарского края

№ п/п	Объекты проверки	Результаты проверки	Примечание
1	2	3	4
1.1	Проверка перечня используемых для доступа к АРМ учетных записей пользователей с фактическими, использованными для доступа к АРМ		
1.2	Проверка на АРМ пользователей информации (в том числе в истории Интернет-браузеров), не относящейся к служебным обязанностям		
1.3	Проверка состава, используемого на АРМ пользователей программного обеспечения (в соответствии с Реестром разрешённого к использованию ПО)		
1.4	Проверка наличия печатей (пломб) на АРМ		
1.5	Проверка наличия установленных на АРМ паролей		

	на доступ к BIOS		
1	2	3	4
1.6	Проверка возможности использования на АРМ пользователей технологий беспроводной передачи данных, веб-камер и микрофонов		
1.7	Проверка работоспособности на АРМ и серверах средств защиты информации		
1.8	Проверка настроек программного обеспечения и средств защиты информации требованиям эксплуатационной документации		Проверяется в том числе актуальность антивирусных баз
1.9	Проверка АРМ и серверов на предмет подключения к ним мобильных устройств передачи информации (в ретроспективе), а также неучтенных съемных носителей информации		
2	Учет и использование съемных носителей информации		
1.2	Проверка наличия перечня мест хранения съемных носителей, назначения ответственных за них лиц и степени их актуальности		
2.2	Проверка съемных носителей информации на предмет наличия информации, не связанной с использованием служебных обязанностей		
1.3	Проверка выполнения уничтожения (стирания) информации со съемных носителей информации		
2.3	Проверка выполнения порядка уничтожения съемных носителей информации		
3	Использование аутентификационной информации при доступе к информационным активам		

1	2	3	4
3.1	Выборочная проверка реализации требований, установленных к качеству аутентификационной информации и мер по обеспечению ее безопасности		После проверок исполнения требований к качеству пароля (приводящие к его санкционированной компрометации), пользователь должен продемонстрировать установленный пароль на доступ, после чего незамедлительно его сменить
3.2	Отсутствие сохраненных паролей доступа как средствами программного обеспечения, так и на бумажных носителях (вне отведенных для этого мест)		
4	Организация доступа в помещения обработки информации и выполнение требований, установленных к таким помещениям		
4.1	Проверка наличия перечня лиц, допущенных в помещения обработки конфиденциальной информации, степени его актуальности		Проверка наличия перечня для каждого помещения, а также в ходе проведения аудита - проверяется степени исполнения данного требования при доступе в помещения
4.2	Проверка наличия перечня мест хранения материальных носителей персональных данных и ответственных, степени актуальности данного перечня		
5	Учет и использование средств криптографической защиты информации		
5.1	Проверка условий эксплуатации СКЗИ, в том числе выполнение требований эксплуатационной		

	документации на СКЗИ		
1	2	3	4
5.2	Проверка ознакомления работников с нормативными документами, регламентирующими процессы обработки и защиты информации (в том числе персональных данных)		Может проводить в формате тестирования или анкетирования с установленным перечнем контрольных вопросов

Начальник управления информатизации и
информационной безопасности

Н.Н.Сергиевская