Приложение 2
к Регламенту расчета показателя состояния технической защиты информации в информационных системах администрации муниципального образования Северский муниципальный район Краснодарского края

Форма расчета показателя состояния защищенности

Расчет произведен для объекта информатизации: _____

Номер группы показателей (j)	**Наименование групп показателей**	**Номер (i) и наименование частного показателя безопасности (частного показателя k_{ji})**	**Значение частного показателя безопасности (частного показателя k_{ji})**	**Значение весового коэффициент группы показателей (R_j)**	**Оценка выполнения (Да – 1 / Нет -0)**	**Расчет**
1	Организация и управление	1. На заместителя руководителя органа (организации) возложены полномочия ответственного лица за обеспечение информационной безопасности органа (организации) и определены его обязанности	0,30	0,10		
		2. Определены функции (обязанности) структурного подразделения (или отдельных работников), ответственного за обеспечение информационной безопасности органа (организации)	0,40			

Номер группы показателей (j)	**Наименование групп показателей**	**Номер (i) и наименование частного показателя безопасности (частного показателя k_{ji})**	**Значение частного показателя безопасности (частного показателя k_{ji})**	**Значение весового коэффициент группы показателей (R_j)**	**Оценка выполнения (Да – 1 / Нет -0)**	**Расчет**
		3. К подрядным организациям, имеющим доступ к информационным системам с привилегированными правами, в договорах установлены требования о реализации мер по защите от угроз через информационную инфраструктуру подрядчика	0,30			
2	Защита пользователей	1. Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике. В случае отсутствия технической возможности обеспечения требуемой сложности паролей реализованы компенсирующие меры	0,30	0,25		
		2. Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)	0,30			
		3. Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию	0,20			
		4. Отсутствуют активные учетные записи работников органа (организации) и работников, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения	0,20			
3	Защита	1. На сетевом периметре информационных систем	0,20	0,35		

Номер группы показателей (j)	**Наименование групп показателей**	**Номер (i) и наименование частного показателя безопасности (частного показателя k_{ji})**	**Значение частного показателя безопасности (частного показателя k_{ji})**	**Значение весового коэффициент группы показателей (R_j)**	**Оценка выполнения (Да – 1 / Нет -0)**	**Расчет**
	информационных систем	установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет, контролируется межсетевыми экранами уровня L3/L4)				
		2. На устройствах и интерфейсах, доступных из сети Интернет, отсутствуют уязвимости критического уровня опасности с датой публикации обновлений (компенсирующих мер по устранению) в банке данных угроз ФСТЭК России, на официальных сайтах разработчиков, иных открытых источниках более 30 дней или в отношении таких уязвимостей реализованы компенсирующие меры	0,25			
		3. На пользовательских устройствах и серверах отсутствуют уязвимости критического уровня с датой публикации обновления (компенсирующих мер по устранению) более 90 дней (не менее 90% устройств и серверов) или в отношении таких уязвимостей реализованы компенсирующие меры	0,15			
		4. Обеспечена проверка вложений в электронных письмах электронной почты на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств)	0,15			
		5. Обеспечено централизованное управление средствами антивирусной защиты (не менее чем 80% пользовательских устройств и серверов контролируются средствами антивирусной	0,15			

Номер группы показателей (j)	**Наименование групп показателей**	**Номер (i) и наименование частного показателя безопасности (частного показателя k_{ji})**	**Значение частного показателя безопасности (частного показателя k_{ji})**	**Значение весового коэффициент группы показателей (R_j)**	**Оценка выполнения (Да – 1 / Нет -0)**	**Расчет**
		защиты с централизованным управлением). При этом обеспечены контроль и установка обновлений баз данных признаков вредоносного программного обеспечения не реже чем 1 раз в месяц				
		6. Реализована очистка входящего из сети Интернет сетевого трафика от компьютерных атак, направленных на отказ в обслуживании, на уровне L3/L4 (заключен договор с провайдером)	0,10			
4	Мониторинг информационной безопасности и реагирование	1. Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей	0,40	0,30		
		2. Реализован централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с сетью Интернет	0,35			
		3. Утвержден документ, определяющий порядок реагирования на компьютерные инциденты	0,25			
Значение показателя защищенности				Кзи		

Расчет произведен:

_____	_____	_____
(должность)	(подпись)	(И.Фамилия)
_____	_____	_____
(должность)	(подпись)	(И.Фамилия)
_____	_____	_____
(должность)	(подпись)	(И.Фамилия)

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская