

Приложение 1

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

Документы и материалы, подтверждающие результаты расчета показателя защищенности

№ п/ п	Частный показатель безопаснос ти	Подтверждающие документы и материалы, на основании которых показателю присваивается значение	Необходимость представления документов во ФСТЭК России
1	k ₁₁	1. Утвержденное главой муниципального образования Северский муниципальный район Краснодарского края распоряжение о назначении заместителя главы администрации муниципального образования Северский муниципальный район Краснодарского края ответственным за организацию работ по информационной безопасности.	Представляется по запросу
		2. Должностной регламент (инструкция) или иной документ, определяющий должностные обязанности (трудовые функции) по обеспечению информационной безопасности заместителя главы администрации муниципального образования Северский район Краснодарского края, ответственного за организацию работ по информационной безопасности	Представляется по запросу
2	k ₁₂	Утвержденное главой муниципального образования Северский район Краснодарского края положение о структурном подразделении по обеспечению информационной безопасности или распоряжение о возложении обязанностей по обеспечению информационной безопасности на отдельных сотрудников, содержащее обязанности (трудовые функции) сотрудников структурного подразделения по обеспечению информационной безопасности или обязанности (трудовые функции), инструкции отдельных сотрудников по обеспечению информационной безопасности	Представляется по запросу
3	k ₁₃	Договор (контракт, выписка, техническое задание или иной документ), на основании которого привлекаемые подрядные организации (при их наличии) имеют доступ к информационным системам, содержащий требования по реализации в инфраструктуре подрядчика мер по защите информации	Представляется по запросу

№ п/ п	Частный показатель безопаснос ти	Подтверждающие документы и материалы, на основании которых показателю присваивается значение	Необходимость представления документов во ФСТЭК России
4	k ₂₁	1. Утвержденное главой муниципального образования Северский муниципальный район Краснодарского края распоряжение, определяющее парольную политику, содержащий требования к длине, периодичности смены и содержанию паролей учетных записей пользователей информационных систем. <u>Минимальные требования:</u> пароль должен содержать не менее 12 символов, буквы верхнего и нижнего регистра (А-Я, А-Z, а-я, а-z), специальные символы (!, », №, %, *, /), в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов).	Представляется по запросу
		2. Снимок экрана, отображающий установленные на средстве обработки информации реализации парольной политики настройки для паролей учетных записей пользователей, подтверждающий соответствие настроек паролей учетных записей пользователей парольной политике.	Представляется с результатами оценки
		3. Отчет, сформированный средством анализа защищенности или иным инструментальным средством, позволяющим выявить пароли, не соответствующие установленным требованиям.	Представляется с результатами оценки
		В случае отсутствия технической возможности выполнения требований к паролям подтверждающим документом является перечень реализованных в информационной системе компенсирующих мер, и материалы, подтверждающие их реализацию	
5	k ₂₂	1. Сведения о программном, программно-аппаратном средстве обработки информации (снимок экрана панели управления средства), с использованием которого осуществляется многофакторная аутентификация привилегированных пользователей.	Представляется с результатами оценки
		2. Сведения о количестве привилегированных пользователей (которые осуществляют удаленное подключение), а также о количестве привилегированных пользователей, в отношении которых реализована многофакторная аутентификация.	Представляется по запросу
		В случае отсутствия технической возможности использования второго фактора аутентификации подтверждающим документом является перечень реализованных компенсирующих мер и материалы, подтверждающие их реализацию	
6	k ₂₃	1. Снимок экрана, отображающий установленные на средстве обработки информации реализации парольной защиты (политики) настройки сброса пароля после первой аутентификации для используемых в информационной системе сервисных учетных записей и учетных записей разработчиков.	Представляется с результатами оценки
		2. Отчет, сформированный средством анализа	Представляется

№ п/ п	Частный показатель безопаснос ти	Подтверждающие документы и материалы, на основании которых показателю присваивается значение	Необходимость представления документов во ФСТЭК России
		защищенности или иным инструментальным средством, позволяющим выявить установленные по умолчанию пароли учетных записей пользователей.	с результатами оценки
7	k ₂₄	Утвержденное главой муниципального образования Северский муниципальный район Краснодарского края распоряжение, содержащее требования о необходимости удаления (отключения) учетных записей сотрудников с которыми прекращены трудовые или иные отношения.	Представляется по запросу
8	k ₃₁	1. Перечень интерфейсов (IP-адреса, доменные имена, физические интерфейсы (порты)), доступных из сети «Интернет».	Представляется по запросу
		2. Сведения о применяемых средствах межсетевого экранирования уровня L3/L4 и снимки экрана панели управления средств межсетевого экранирования, содержащие настройки правил доступа к сервисам (службам), доступным из сети «Интернет».	Представляется с результатами оценки
		В случае отсутствия в информационной системе сервисов (служб) доступных из сети «Интернет» (отсутствие взаимодействия с сетью «Интернет») подтверждающим документом являются сведения об их отсутствии.	
9	k ₃₂	1. Сведения о количестве устройств и перечень интерфейсов, доступных из сети «Интернет».	Представляется по запросу
		2. Отчет, сформированный средством анализа защищенности, содержащий результаты сканирования устройств и интерфейсов, доступных из сети «Интернет», на наличие уязвимостей уровня «критический» (с датой сканирования не ранее 30 дней даты проведения оценки).	Представляется с результатами оценки
		3. Перечень реализованных компенсирующих мер, в случае отсутствия технической возможности устранения уязвимостей уровня «критический», и материалы, подтверждающие их реализацию	Представляется по запросу
10	k ₃₃	1. Сведения о количестве пользовательских устройств и серверов.	Представляется по запросу
		2. Отчет, сформированный средством анализа защищенности, содержащий результаты сканирования пользовательских устройств и серверов на наличие уязвимостей уровня «критический».	Представляется с результатами оценки
		3. Перечень реализованных компенсирующих мер, в случае отсутствия технической возможности устранения уязвимостей уровня «критический», и материалы, подтверждающие их реализацию.	Представляется по запросу
11	k ₃₄	1. Сведения, содержащие общее количество автоматизированных рабочих мест и количество автоматизированных рабочих мест, на которых осуществляется проверка почтовых вложений средствами	Представляется по запросу

№ п/ п	Частный показатель безопаснос ти	Подтверждающие документы и материалы, на основании которых показателю присваивается значение	Необходимость представления документов во ФСТЭК России
		антивирусной защиты. 2. Сведения о применяемых средствах антивирусной защиты (снимок экрана панели управления средством). 3. Отчет, сформированный средством антивирусной защиты, используемом для защиты электронной почты, содержащий сведения о количестве устройств, на которых функционируют средства антивирусной защиты, обеспечивающие проверку вложений в электронных письмах электронной почты на наличие вредоносного программного обеспечения. <u>В случае отсутствия электронной почты в информационных системах подтверждающим документом являются сведения об ее отсутствии.</u>	Представляется с результатами оценки Представляется по запросу
12	k ₃₅	1. Сведения, содержащие общее количество автоматизированных рабочих мест, функционирующих в органе (организации). 2. Снимок экрана страницы настройки средства централизованного управления антивирусной защиты информации, отображающий количество автоматизированных рабочих мест, которые находятся под его управлением. 3. Отчет, сформированный средством централизованного управления антивирусной защиты информации, содержащий: дату последних обновлений средств антивирусной защиты на каждом объекте защиты (на автоматизированных рабочих местах, серверах, мобильных устройствах, подключенных к средству централизованного управления антивирусной защиты); дату последней проверки на автоматизированных рабочих местах, серверах, мобильных устройствах, подключенных к средству централизованного управления антивирусной защиты	Представляется по запросу Представляется с результатами оценки Представляется по запросу
13	k ₃₆	Копия договора (выписки) с оператором связи (иной организацией), в который включены работы по очистке входящего из сети «Интернет» трафика на уровне L3/L4. <u>В случае самостоятельной блокировки</u> входящего сетевого трафика подтверждающим документом являются сведения о применяемых методах и средствах защиты от атак типа «отказ в обслуживании». <u>В случае отсутствия</u> веб-сайтов, служб или иных сервисов, доступных из сети «Интернет» и подлежащих защите подтверждающим документом являются сведения, предусмотренные для показателя k₃₁	Представляется с результатами оценки
14	k ₄₁	1. Сведения о количестве привилегированных учетных	Представляется по

№ п/ п	Частный показатель безопаснос ти	Подтверждающие документы и материалы, на основании которых показателю присваивается значение	Необходимость представления документов во ФСТЭК России
		записей пользователей, и перечень событий информационной безопасности, в отношении которых осуществляется сбор информации.	запросу
		2. Снимок экрана с вкладки настроек системы (средства) мониторинга информационной безопасности, отображающий установленные настройки оповещения о неудачных попытках входа для всех привилегированных учетных записей.	Представляется с результатами оценки
		3. Отчет, сформированный системой (средством) мониторинга информационной безопасности, содержащий сведения о зарегистрированных ранее событиях информационной безопасности.	Представляется по запросу
15	k ₄₂	1. Перечень регистрируемых событий информационной безопасности и сведения о количестве автоматизированных рабочих мест, с которых осуществляется доступ в сеть «Интернет.	Представляется по запросу
		2. Снимок экрана с вкладки настроек системы (средства) мониторинга информационной безопасности, отображающий количество автоматизированных рабочих мест, с которых осуществляется централизованный сбор событий безопасности.	Представляется с результатами оценки
		3. Отчет, сформированный системой (средством) мониторинга информационной безопасности, содержащий сведения о зарегистрированных ранее событиях информационной безопасности.	Представляется по запросу
16	k ₄₃	Утвержденное главой муниципального образования Северский муниципальный район Краснодарского края распоряжение, определяющее порядок реагирования на компьютерные инциденты	Представляется по запросу

Начальник управления информатизации
и информационной безопасности

Н.Н.Сергиевская