Реализация рекомендаций ФСТЭК России по повышению защищенности информационных (автоматизированных) систем, в которых функционируют операционные системы Linux

1. Установить (в случае наличия использовать) средства антивирусной защиты на всех серверах и автоматизированных рабочих местах, функционирующих в информационной инфраструктуре органа (организации). Провести контроль установки указанных средств, а также обеспечить ежедневное обновление их антивирусных баз

№ п/п	Наименование средства антивирусной защиты	Количество устройств (серверы, АРМ), на которых установлены средства антивирусной защиты	Количество устройств (серверы, АРМ), на которых не установлены средства антивирусной защиты
1	...	...	...

2. Проводить периодическое полное сканирование информационной инфраструктуры органа (организации), в том числе входящих в ее состав операционных систем Linux, с использованием сертифицированных средств антивирусной защиты.

№ п/п	Количество просканированных узлов информационной инфраструктуры	Сведения о выявленном вредоносном программном обеспечении
1	...	...

3. Реализовать Рекомендации по безопасной настройке операционных систем Linux, утвержденные ФСТЭК России 25 декабря 2022 г. (указанные рекомендации размещены на официальном сайте ФСТЭК России по адресу – https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-25-dekabrya-2022-g).

№ п/п	Наименование операционной системы	Количество узлов информационной инфраструктуры, на которых произведена настройка операционной системы
1	...	...

4. Использовать системы мониторинга событий информационной безопасности. В случае их отсутствия - организовать применение доступных систем мониторинга (например, auditd, osquery). Произвести корректную настройку логирования действий пользователей на узлах сети под управлением

операционных систем Linux. Запись действий пользователей должна осуществляться с указанием временных меток.

№ п/п	Наименование применяемой системы мониторинга событий информационной безопасности	Информация о внедрении доступных систем мониторинга событий (в случае отсутствия системы мониторинга)
1	...	...

5 Исключить доступ к информационной инфраструктуре органа (организации) привилегированных пользователей по протоколу удаленного доступа SSH, в том числе аутентификации пользователя root. В случае невозможности, настроить аутентификацию пользователей по SSH-ключам.

№ п/п	Количество внешних интерфейсов, используемых для удаленного подключение к информационной инфраструктуре органа (организации)	Используемые протоколы для удаленного доступа к информационной инфраструктуре органа (организации)	Сведения об ограничении использования протокола удаленного доступа SSH
1	...	...	...

6. Обновить системное и прикладное программное обеспечение, применяемое в информационной инфраструктуре органа (организации) в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (указанный документ размещен на официальном сайте ФСТЭК России по адресу — https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g).

№ п/п	Сведения об обновлении системного и прикладного программного обеспечения	Причины невозможности обновления (при наличии)
1	...	...

7. Организовать двухфакторную аутентификацию внешних пользователей (подрядчиков, обеспечивающих в том числе функционирование информационной инфраструктуры), а также для всех внутренних привилегированных пользователей.

№ п/п	Информация о применяемых методах двухфакторной аутентификации	Сведения о реализации двухфакторной аутентификации для внешних и внутренних пользователей
1	...	...

8 Организовать сегментирование информационной инфраструктуры и ограничить доступ пользователей к таким сегментам с учетом выполняемых ими задач (бизнес-процессов) в органе (организации) с применением средств межсетевого экранирования.

№ п/п	Сведения о наличии сегментов в информационной инфраструктуре органа (организации)	Сведения об организации сегментирования информационной инфраструктуры	Сведения о причинах невозможности организации сегментирования информационной инфраструктуры
1	...	...	...

9 Исключить использование иностранных DNS-серверов. Использовать для обеспечения функционирования информационной инфраструктуры органа (организации) публичные резолверы национальной системы доменных имен (по возможности). В этих целях необходимо внести изменения в список DNS-серверов для конечного клиента следующую информацию, которая содержится в таблице:

	a.res-nsdi.ru	*b.res-nsdi.ru*
ipv4	*195.208.4.1*	*195.208.5.1*
ipv6	*2a0c:a9c7:8::1*	*2a0c:a9c7:9::1*

№ п/п	Сведения о применяемых в информационной инфраструктуре DNS-серверах	Сведения об использовании в информационной инфраструктуре публичные резолверов национальной системы доменных имен
1	...	...

10. Ограничить доступ к командной строке операционной системы для всех пользователей информационной инфраструктуры органа (организации), за исключением администраторов безопасности и системных администраторов.

№ п/п	Сведения об ограничении доступа к командной строке для всех пользователей	Количество хостов информационной инфраструктуры, на которых ограничен доступ к командной строке

	информационной	операционной системы
1	...	...

11. Провести анализ сетевых подключений на предмет наличия сервисов динамических имен (Dynamic DNS). По возможности отказаться от использования указанных сервисов.

№ п/п	Сведения об использовании сервисов динамических имен	Количество хостов информационной инфраструктуры, на которых используются сервисы динамических имен
1	...	...

12. Провести сканирование информационной инфраструктуры на наличие индикаторов компрометации и yara-правилами с использованием специализированных программных инструментов (при наличии), либо другого доступного программного обеспечения (например, YARA, Loki Scan). Индикаторы компрометации содержатся в отчете экспертного центра Позитив Текнолоджиз, доступном по адресу — https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/hellhounds-operaciya-lahat/.

№ п/п	Количество просканированных узлов информационной инфраструктуры	Сведения о выявленных индикаторах компрометации
1	...	...

По результатам выполнения указанных рекомендаций просим проинформировать Управление ФСТЭК России по Центральному федеральному округу, по представленной форме до 22 декабря 2023 г.