УДК 004.056

Баженов Михаил Сергеевич магистрант
2 курс, СПбГУТ им. проф. М. А. Бонч-Бруевича
Россия, г. Санкт-Петербург
Алексеева Ксения Евгеньевна магистрант
2 курс, СПбГУТ им. проф. М. А. Бонч-Бруевича
Россия, г. Санкт-Петербург

АДАПТАЦИЯ МЕТОДИКИ ПЕРВИЧНОГО АУДИТА ASTRA LINUX ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ ПОЧТОВЫХ СЛУЖБ

Аннотация: *Показано, как методику первичного аудита Astra Linux, работающую в режиме чтения, можно распространить на почтовые службы. Для связки протоколов передачи и доступа к ящикам выделены проверяемые характеристики: состояние портов почтовых протоколов, обязательность шифрования канала, ограничение пересылки чужих сообщений, права на файлы настройки, состав сервисов и полнота журналирования. На их основе составлен набор проверок почтового узла с указанием уровня критичности и приведен пример блока данных в формате JSON. Установлено, что событийная балльная оценка переносится на почтовые службы без изменения порядка расчета, что говорит о расширяемости методики.*

Ключевые слова: *Astra Linux, почтовый узел, протокол передачи, доступ к ящикам, шифрование канала, проверки, показатель риска*

Annotation: *It is shown how the read-mode Astra Linux primary audit methodology can be extended to mail services. For the message transfer and mailbox access stack the verifiable characteristics are identified: the state of mail protocol ports, mandatory channel encryption, restriction of relaying of foreign messages, configuration file permissions, the set of services and logging completeness. On this*

basis a set of mail host checks with criticality levels is compiled, and an example JSON data block is given. The event-based scoring is found to transfer to mail services without changing the calculation order, which indicates the extensibility of the methodology.

Key words: *Astra Linux, mail host, transfer protocol, mailbox access, channel encryption, checks, risk indicator*

Введение

Почтовый узел остается одним из наиболее значимых и одновременно наиболее уязвимых элементов корпоративной инфраструктуры. На платформе Astra Linux почтовые службы строятся из типовых компонентов передачи сообщений и доступа к ящикам, поэтому к ним применимы общие правила первичной проверки настройки. Вместе с тем почтовый узел несет собственные источники риска, связанные с протоколами передачи и доступа, и это требует дополнения каталога проверок.

Задача работы состоит в распространении ранее предложенной методики первичного аудита на область почтовых служб: в выделении проверяемых характеристик для протоколов передачи и доступа к ящикам и в составлении набора проверок почтового узла в рамках общей событийной оценки риска.

Проверяемые характеристики почтового узла

Набор собираемых характеристик дополняется почтовым блоком. Агент в режиме чтения фиксирует состояние портов почтовых протоколов, обязательность шифрования клиентских и межсерверных соединений, ограничение пересылки чужих сообщений, владельцев и режимы файлов настройки почтовых служб, состав запущенных и автозапускаемых сервисов и полноту журналирования почтовых событий. Перечень характеристик приведен в таблице 1.

Таблица 1.

Характеристики первичной проверки почтового узла

Характеристика	Что проверяется	Значение для безопасности
Порты протоколов	открытость и доступность портов передачи и доступа	сетевая поверхность почтовой службы
Шифрование канала	защита клиентских и межсерверных соединений	защита учетных данных и содержимого
Пересылка сообщений	ограничение пересылки чужих сообщений	риск открытого ретранслятора и рассылок
Файлы настройки	владелец и режим файлов служб	защита настроек от подмены
Состав сервисов	запущенные и автозапускаемые службы	соответствие профилю почтового узла
Журналирование	наличие и полнота почтовых журналов	наблюдаемость и расследование инцидентов

Все характеристики собираются без воздействия на службу: агент читает файлы настройки и состояние сервисов, но не отправляет пробных сообщений и не проверяет пересылку активными способами. Тем самым сохраняется принцип чтения, а проверка остается безопасной для действующего почтового узла.

Набор проверок почтового узла

На основе характеристик составлен набор проверок почтовой области в рамках общей балльной оценки. Каждой проверке присвоен вес по шкале от единицы до десяти соответственно уровню критичности. Состав проверок дан в таблице 2.

Таблица 2.

Набор проверок почтового узла

Код	Условие срабатывания	Уровень	Вес
MAIL-001	разрешена пересылка чужих сообщений	критический	10
MAIL-002	клиентский вход без обязательного шифрования	высокий	8

MAIL-003	доступ к ящикам без шифрования канала	высокий	8
MAIL-004	ослабленные права на файлы настройки	средний	5
MAIL-005	почтовый сервис вне профиля в автозапуске	средний	4
MAIL-006	неполное журналирование почтовых событий	низкий	2

Разрешенная пересылка чужих сообщений отнесена к критическому уровню, поскольку позволяет применять узел для рассылок и подрывает доверие к домену. Отсутствие обязательного шифрования и доступ к ящикам без защиты канала отнесены к высокому уровню из-за угрозы перехвата учетных данных и переписки. Ослабленные права на файлы настройки и лишние сервисы отнесены к среднему уровню, а неполное журналирование к низкому, так как оно ухудшает наблюдаемость без немедленного захвата. Уровни согласуются с практиками защиты удаленного доступа и контроля настройки [1; 2].

Представление данных и обсуждение

Почтовые характеристики включаются в общий документ узла. В блоке почтовых данных предусмотрены поля для перечня обнаруженных портов, признака обязательного шифрования, признака разрешенной пересылки, режима доступа к файлам настройки и признака полноты журналирования. Единый формат сохраняет применимость прежнего анализатора и прежнего порядка расчета: базовый риск равен сумме весов сработавших проверок, итоговый показатель приводится к стобалльной шкале, а повторы, например несколько сервисов вне профиля, учитываются по отдельности.

Перенос методики на почтовые службы подтверждает ее расширяемость, поскольку добавление новой области не меняет ядро расчета. Ограничением остается то, что первичная проверка фиксирует характеристики настройки, но не

выполняет активной проверки пересылки и не анализирует содержимое потока сообщений, что относится к задачам специализированных средств защиты почты [3].

Заключение

Предложено распространение методики первичного аудита Astra Linux на почтовые службы. Выделены проверяемые характеристики для протоколов передачи и доступа к ящикам, составлен набор проверок почтового узла с указанием уровня критичности и показан пример представления данных. Установлено, что событийная балльная оценка переносится без изменения порядка расчета. Развитие связано с профилями почтового узла и со связкой первичной проверки с контролем доменных политик подлинности отправителя.

Использованные источники:

1. Операционная система Astra Linux Special Edition. Эксплуатационная документация // Справочный центр Astra Linux. URL: https://wiki.astralinux.ru/ (дата обращения: 21.06.2026).

2. CIS Critical Security Controls Version 8.1 [Электронный ресурс]. URL: https://www.cisecurity.org/controls/v8-1 (дата обращения: 21.06.2026).

3. NIST SP 800-45 Version 2. Guidelines on Electronic Mail Security [Электронный ресурс]. URL: https://csrc.nist.gov/publications/detail/sp/800-45/version-2/final (дата обращения: 21.06.2026).

4. RFC 5321. Simple Mail Transfer Protocol / J. Klensin. IETF, 2008 [Электронный ресурс]. URL: https://www.rfc-editor.org/info/rfc5321 (дата обращения: 21.06.2026).

5. RFC 3207. SMTP Service Extension for Secure SMTP over Transport Layer Security / P. Hoffman. IETF, 2002 [Электронный ресурс]. URL: https://www.rfc-editor.org/info/rfc3207 (дата обращения: 21.06.2026).

6. Common Vulnerability Scoring System v3.1: Specification Document / FIRST [Электронный ресурс]. URL: https://www.first.org/cvss/v3.1/specification-document (дата обращения: 21.06.2026).

7. Linux man-pages: sshd_config(5) [Электронный ресурс]. URL: https://man7.org/linux/man-pages/man5/sshd_config.5.html (дата обращения: 21.06.2026).

8. Postfix: official documentation / The Postfix Project [Электронный ресурс]. URL: https://www.postfix.org/documentation.html (дата обращения: 21.06.2026).

9. Dovecot: documentation / Open-Xchange [Электронный ресурс]. URL: https://doc.dovecot.org/ (дата обращения: 21.06.2026).

10. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_378330/ (дата обращения: 21.06.2026).