Postfix: SSL_accept error и TLS library problem

В логах была замечена ошибка:

```
Jan 29 00:53:20 mail postfix/smtpd[73728]: SSL_accept error from pirate.census.shodan.io[71.6.146.185]: -1
Jan 29 00:53:20 mail postfix/smtpd[73728]: warning: TLS library problem: error:1408A10B:SSL routines:ssl3_get_client_hello:wrong version number:/usr/src/crypto/openssl/ssl/s3_srvr.c:969:
```

что указывает на проблемы версии openssl. Проверка:

```
# openssl s_client -starttls smtp -crlf -connect mail.tst-amo.net.ua:587 -ssl3
CONNECTED(00000003)
34380880456:error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure:/usr/src/crypto/openssl/ssl/s3_pkt.c:1498:SSL alert number 40
34380880456:error:1409E0E5:SSL routines:ssl3_write_bytes:ssl handshake failure:/usr/src/crypto/openssl/ssl/s3_pkt.c:659:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 216 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : SSLv3
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
```

```
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1548750442
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```

Теперь без указания версии:

```
# openssl s_client -starttls smtp -crlf -connect mail.tst-
amo.net.ua:587
........
    Start Time: 1548750495
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
250 SMTPUTF8
```

Смотрим настройки postfix:

```
smtp_tls_mandatory_ciphers = high
smtp_tls_protocols=!SSLv2,!SSLv3
smtp_tls_mandatory_protocols=!SSLv2,!SSLv3
tls_high_cipherlist = ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
AES256-GCM-SHA384:DHE-RSA-AES128-GCM-S
HA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-
SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA
384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-
ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-
DSS-AES128-SHA256:DHE-RSA-AES256-SHA256
:DHE-DSS-AES256-SHA:DHE-RSA-AES256-
SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK
smtpd_tls_mandatory_ciphers = high
smtpd_tls_mandatory_protocols=!SSLv2,!SSLv3
smtpd_tls_protocols=!SSLv2,!SSLv3
```