УТВЕРЖДАЮ
Руководитель компании ООО «АВС» А.Б. Петров
____ _____2024 г.

Экз. №1

Политика аутентификации для личного кабинета «Партнера-API»

1. Цель настоящей политики является обеспечение безопасного удаленного подключения партнеров и пользователей компании «АВС» к административному интерфейсу.

2. Термины и определения:
Аутентификация – процесс проверки пользователя партнера для осуществления легитимных действий в системе.
Многофакторная аутентификация – процесс проверки прав доступа партнера через 2 и более механизма аутентификации.
Партнер – физическое или юридическое лицо, имеющее доступ к системе «Партнер – API».

3. Основные положения к безопасному удалённому подключению системы «Партнер – API» основаны на ГОСТ Р 57580.1 2017 в части касающейся парольной политики и техники защиты информации кредитно-финансовой организации, а также требования PCI DSS 4.0 в части касающейся защиты карточных данных пользователей.

3.1 Безопасность паролей:

- пароль учетной записи «Партнер – API» должен содержать не менее 12 символов содержащий заглавные буквы, цифры, а также символы (верхний-нижний регистры);
- смена паролей должна происходить каждые 60 календарных суток;
- запрещается использовать пароли от учетной записи содержащиеся в списке запрещенных паролей[1]
- допускается генерация паролей в сторонних сервисах, после фиксации пароля.

3.2. Учетная запись пользователя «Партнер – API»

- блокировка учетной записи наступает при 5 неуспешных попыток аутентификации сроком на 30 минут.

[1] Список запрещенных паролей от 10.01.2024 (постоянно обновляющийся документ в организации)

- в случае неактивной сессии учетной записи при успешной аутентификации, сессия будет прервана через 15 минут;

- удаление учетной записи происходит при прекращении кредитно-финансовых связей пользователя «Партнер- API» с организацией «АВС»

3.3. Многофакторная аутентификация

- помимо стандартной парольной политики в организации «АВС», используется многофакторная аутентификация включающая в себя получения токена по зарегистрированному номеру телефона учетной записи в системе «Партнер - API»;

- при неуспешном вводе токена, он будет направлен повторно.

4. Ответственность за исполнение указанных требований защиты учетной записи системы «Партнер – API» возложить на начальника отдела информационной безопасности Петрова Б.В.

Начальник отдела
информационной безопасности Б.В. Петров
12 июля 2024 г.