Общество с ограниченной ответственностью "АВС"
(ООО "АВС")

УТВЕРЖДАЮ
Председатель правления ООО "АВС"

_____ Иванов А. Г.

23.07.2024

Политика аутентификации для внутреннего административного приложения управления информацией платёжными интеграциями с партнёрами «Партнёр-API»

Москва 23.07.24

1. Общие положения

1.1. Настоящая политика определяет условия процедуры аутентификации сотрудников и партнеров компании в административную панель управления информацией платёжных интеграций с партнёрами «Партнёр-API».

1.2. Политика разработана в соответствии с требованиями регуляторов, ГОСТ 57580 и PCI DSS 4.0.

1.3. Аутентификация сотрудников и партнеров необходима для обеспечения безопасности и конфиденциальности информации, а также для предотвращения несанкционированного доступа к системам и ресурсам компании.

2. Термины и определения

В настоящей политике используются следующие термины и определения:

- Аутентификация - процесс проверки подлинности предъявленного пользователем идентификатора.
- Многофакторная аутентификация (МФА) — метод аутентификации, основанный на использовании двух или более факторов для подтверждения личности пользователя.
- Удалённый доступ — возможность доступа к системе или ресурсу из удалённого места через интернет или другие каналы связи.
- Учётная запись - совокупность сведений о пользователе, необходимая для его аутентификации и предоставления доступа к административной панели.
- Компрометация – факт доступа постороннего лица к данным, а также подозрение на него.

3. Требования к паролям

3.1. Длина пароля должна быть не менее 10 символов.

3.2. Пароль должен содержать буквы верхнего и нижнего регистра, цифры и специальные символы.

3.3. Периодичность смены пароля — каждые 60 дней.

3.4. Запрещается использовать одинаковые пароли для разных учётных записей.

3.5. Запрещается использовать в качестве паролей легко вычисляемые сочетания букв и цифр (например имена, фамилии, даты рождения, наименования, общепринятые сокращения).

3.6. Незамедлительно сменить пароль при компрометации данных.

4. Многофакторная аутентификация

4.1. Для повышения уровня безопасности необходимо использовать двухфакторную аутентификацию с помощью SMS-кода или входящего вызова на мобильный телефон.

4.2. В случае неудачного ввода кода, предусмотреть повторный запрос, он не ранее чем через 5 минут.

4.3. Запрещается использование одних и тех же данных в параллельных сессиях, активная сессия возможна только на одном устройстве.

5. Блокировка учётных записей и автоматическое отключение неактивных сессий

5.1. При трёх неудачных попытках входа в систему учётная запись блокируется на 1 час.

5.2. Неактивные сессии автоматически отключаются через 15 минут бездействия.

5.3. Предусмотреть незамедлительную блокировку учетной записи при прекращении договорных отношений пользователя «Партнер- API» с организацией ООО «АВС».

6. Удалённый доступ

6.1. Удаленный доступ к системе «Партнёр-API» осуществляется только с использованием защищённого соединения связи VPN

6.2. Для удалённого доступа используется двухфакторная аутентификация.

7. Порядок и сроки пересмотра

7.1. Пересмотр настоящей политики осуществляется не реже одного раза в год.

7.2. Основаниями для пересмотра могут быть изменения требований регуляторов, внутренних стандартов компании или условий работы с данными.

8. Ответственность

8.1. Сотрудники, нарушающие требования настоящей политики, могут быть привлечены к дисциплинарной ответственности. В случае несанкционированного доступа к данным компании виновные лица могут быть привлечены к уголовной ответственности.

8.2. Ответственность за техническую часть и подготовку документации для реализации данной политики и исполнения указанных требований возлагается на начальника отдела информационной безопасности — Петрова Б. В.

Начальник отдела
информационной безопасности Петров Б. В.

23.07.2024