Политика аутентификации для внутрненних сервисов

1. Введение

1.1. Цель

Обеспечить надежную идентификацию и аутентификацию во внутренний сервис компании «Партнёр-API», для снижения рисков несанкционированного доступа и использования защищаемых информационных активов.

1.2. Аудитория

С данной политикой должны быть ознакомлены:

- системные администраторы;
- администратор безопасности;
- сотрудники компании.

2. Политика

2.1. Перед обращением к ресурсам системы пользователи должны пройти процедуру идентификации и аутентификации. Успешная идентификация и аутентификация возможна только в случае ввода пользователем правильных аутентификационных данных (как правило, имени пользователя и пароля).
2.2.1. Минимальная длина паролей, которые допускается использовать в приложении – **8** символов. Используемые пароли должны удовлетворять следующим требованиям:

- в пароле должны использоваться символы латинского алфавита верхнего и нижнего регистров, а также цифры (1, 2, 3, 4...) или специальные символы (!, @, #, $…);
- пароль не может повторять **5** ранее использованных;
- пароль не должен основываться на следующих данных:
  - дата рождения, фамилия, имя или отчество пользователя;
  - названия и идентификаторы организации.

2.2.2. Пользователи должны изменять свои пароли не реже, чем раз в **30** дней.
2.3. Для аутентификации пользователей в приложении «Партнёр-API» необходимо использовать двухфакторную аутентификацию с использование мобильного телефона (СМС-код).
2.4. Временная блокировка учетной записи пользователей происходит после выполнения **3** неуспешных последовательных попыток аутентификации на 30 минут.
2.4.1. Срочный процесс восстановления доступа к приложению предусмотрен после личного обращения к администратору и индентификации личности.
2.4.2. Неактивные сессии пользователя отключаются автоматически через 15 минут.
2.5. Доступ к ресурсам организации чётко разграничен и структурирован. Изменения осуществляются по письменному запросу.
2.5.1. Удаленный доступ осуществляется посредством виртуальной частной сети (VPN).

3. Роли и обязанности

Администратор безопасности ООО «АВС»:

- отвечает за претворение в жизнь настоящей политики;
- обеспечивает проведение необходимого обучения;
- осуществляет выбор необходимого набора контрмер и стратегии обеспечения идентификации и аутентификации;
- информирует руководящий аппарат ООО «АВС» о состоянии дел в области обеспечения ИБ и обо всех существенных инцидентах нарушения ИБ;
- осуществляет координацию действий в области обеспечения ИБ;
- проводит контроль за соблюдением требований настоящей политики.

Системные администраторы:

- готовит рекомендации по выбору необходимого набора контрмер и стратегии обеспечения идентификации и аутентификации;

- отвечает за реализацию настоящей политики и соответствующую настройку продуктов ИТ;
- проводит необходимое обучение пользователей на рабочих местах.

Сотрудники выполняют предписанные настоящей политикой мероприятия по обеспечению ИБ.

4. Ответственность за нарушение политики безопасности

4.1. Лица, указанные в разделе 3 настоящей политики, несут персональную ответственность за обеспечение ИБ в соответствии с требованиями настоящей политики безопасности.
4.2. Лица, нарушившие требования безопасности, изложенные в данной политике, совершившие умышленные действия, направленные на нарушение ИБ, могут быть привлечены к дисциплинарной, административной или уголовной ответственности в соответствии с действующим законодательством Российской Федерации.