Типовые ошибки в построении систем аутентификации

Как нельзя хранить пароли?

Открытым текстом

В допускающем расшифровку виде

С применением устаревших хеш-функций
(NTLM, MD5, SHA-1)

Без соли (salt)

А как можно?

Использовать уникальную соль размером не менее 64 бит

Использовать стойкие криптографические хэш-функции

По возможности использовать «медленные» хеш-функции (PBKDF2, scrypt)

Ошибки в реализации формы входа

Неудобный для запоминания логин

Нет шифрования трафика
(http вместо https)

Отсутствие защиты от подбора пароля
или неудачная реализация

Парольный хаос (принуждение пользователя
к многократному вводу паролей)

Парольный хаос

Не предусмотрен вход через соцсети
или плохая реализация

Отсутствует возможность единого входа
(Single Sign-On)

Нет интеграции с входом в корпоративный
домен

Проблемы с формой регистрации

Чрезмерно строгие парольные политики

Отсутствие защиты от массовой регистрации аккаунтов

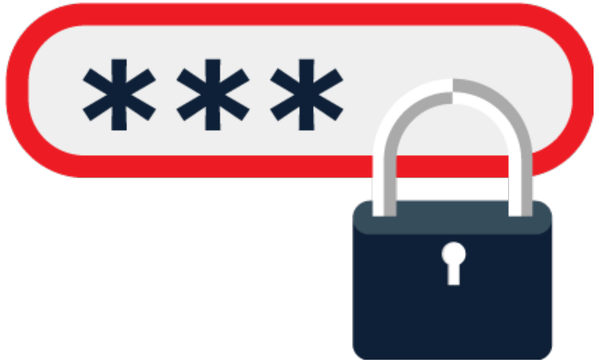
Непродуманное завершение процесса регистрации

… и с восстановлением пароля

Раскрытие информации о пользователе в процессе восстановления

Возможность подбора кода восстановления

Непродуманное завершение процесса восстановления пароля



Недостатки в аудите событий доступа

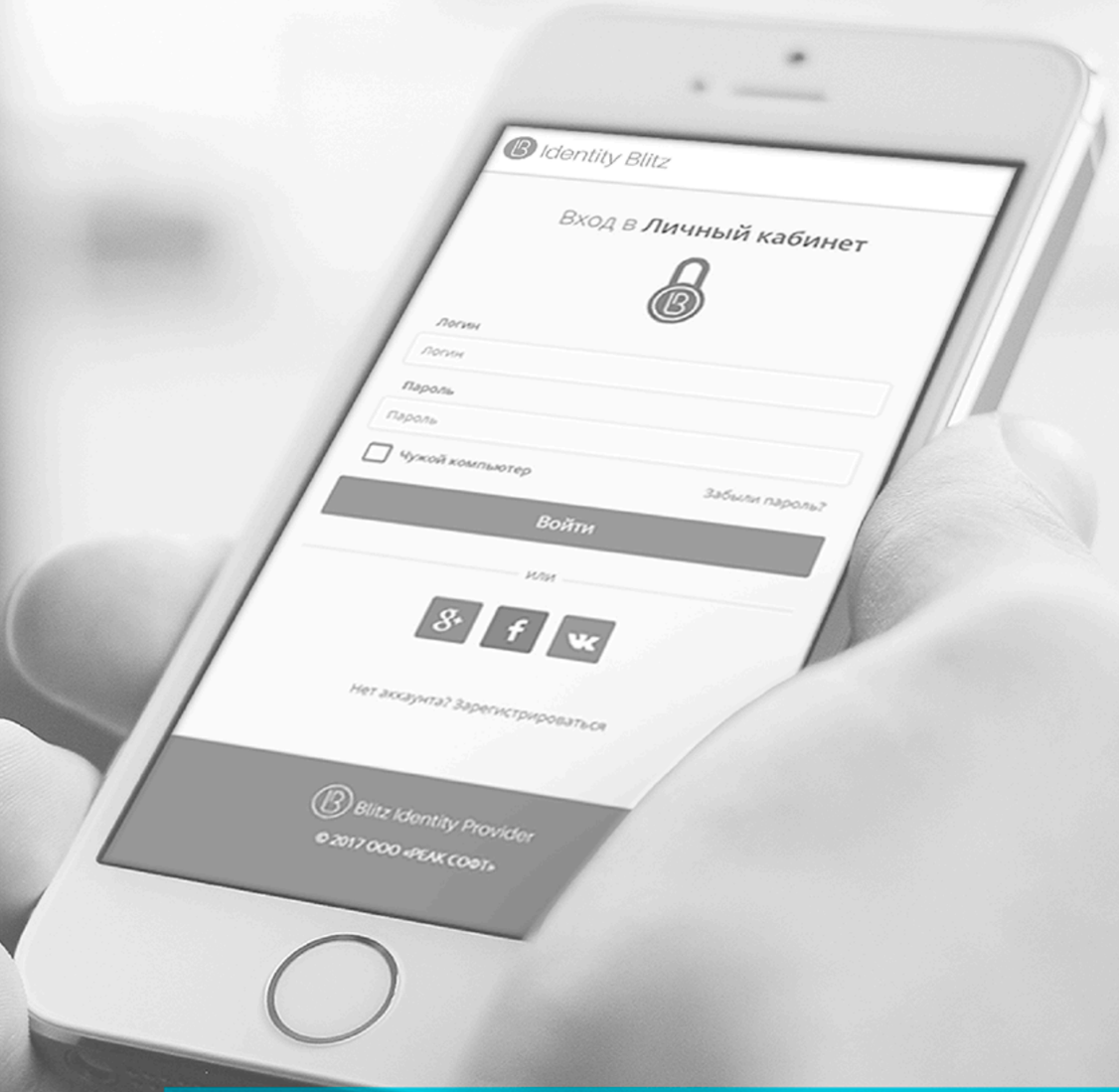
Протоколируется недостаточно информации

Пользователи не информируются о событиях

Не предусмотрены отчеты для администраторов

Blitz Identity Provider

Сервер аутентификации для вашей организации



identityblitz.ru