Защита от использования скомпрометированных электронных почтовых ящиков, паролей и учётных записей

Оглавление

Аутентификация с использованием имени учётной записи (логина) и пароля остается одним из самых популярных и востребованных способов входа в учётную запись пользователя. Сам пароль при этом является **фактором знания.**

Чтобы пароль было проще запомнить, пользователи

- придумывают достаточно простые пароли;
- используют одни и те же учетные данные в разных сервисах.

Это создаёт для злоумышленников дополнительные возможности неправомерного доступа к данным пользователей. Взяв список наиболее распространенных паролей, злоумышленники могут пробовать аутентифицироваться с этими паролями в различные учетные записи в расчете на то, что у кого-то из пользователей окажется один из паролей из списка. Если произошла утечка данных в каком-то стороннем сервисе, то злоумышленники могут взять логины и пароли из утекших данных и попытаться воспользоваться ими для аутентификации в сервисе, являющемся целью атаки, рассчитывая на то, что пользователь используют одинаковые учётные данные на обоих сервисах.

Одной из самых успешных защит от атак такого рода является использование многофакторной аутентификации.

Тем не менее, оправдано создание дополнительных механизмов защиты, которые исключат возможность использования простых словарных паролей или предупредят пользователя о возможной угрозе взлома при использовании одинаковых учетных данных в разных сервисах.

Таким образом, можно выделить две угрозы безопасности пользовательских данных (и два направления возможных атак):

- пользователь использует такие же учетные данные, как и в скомпрометированной учётной записи стороннего сервиса;
- задаваемый пользователем пароль может быть недостаточно сложным или являться широко распространённым;

Предлагаемые решения позволяют значительно снизить значимость таких угроз.

Защита от использования одинаковых учетных данных в разных сервисах

Если учетные данные стороннего сервиса были скомпрометированы, существует риск использования пользователем таких же учетных данных в UIDM.

В данный момент для идентификации скомпрометированных учетных записей UIDM использует адреса электронных почтовых ящиков.

Используя локальный справочник скомпрометированных адресов или API сервиса `haveibeenpwned.com`, UIDM может проверять адреса почтовых ящиков на предмет их наличия в справочнике:

- при выполнении пользователем аутентификации — адреса электронного почтового ящика, указанного в учётной записи такого пользователя;

- с установленной периодичностью — всех существующих в UIDM адресов.

Наличие адреса электронной почты в справочнике скомпрометированных адресов само по себе не означает компрометацию учётной записи UIDM. В зависимости от настроек UIDM реакцией на появление адреса электронной почты пользователя в справочнике скомпрометированных адресов может быть предупреждение пользователя о том, что его учетная запись может быть скомпрометирована, и рекомендация либо требование сменить пароль.

Защита от использования скомпрометированного или простого пароля

При использовании пользователем простого или распространённого пароля для входа в учётную запись в UIDM злоумышленник может получить доступ к профилю пользователя и его персональным данным.

UIDM обеспечивает:

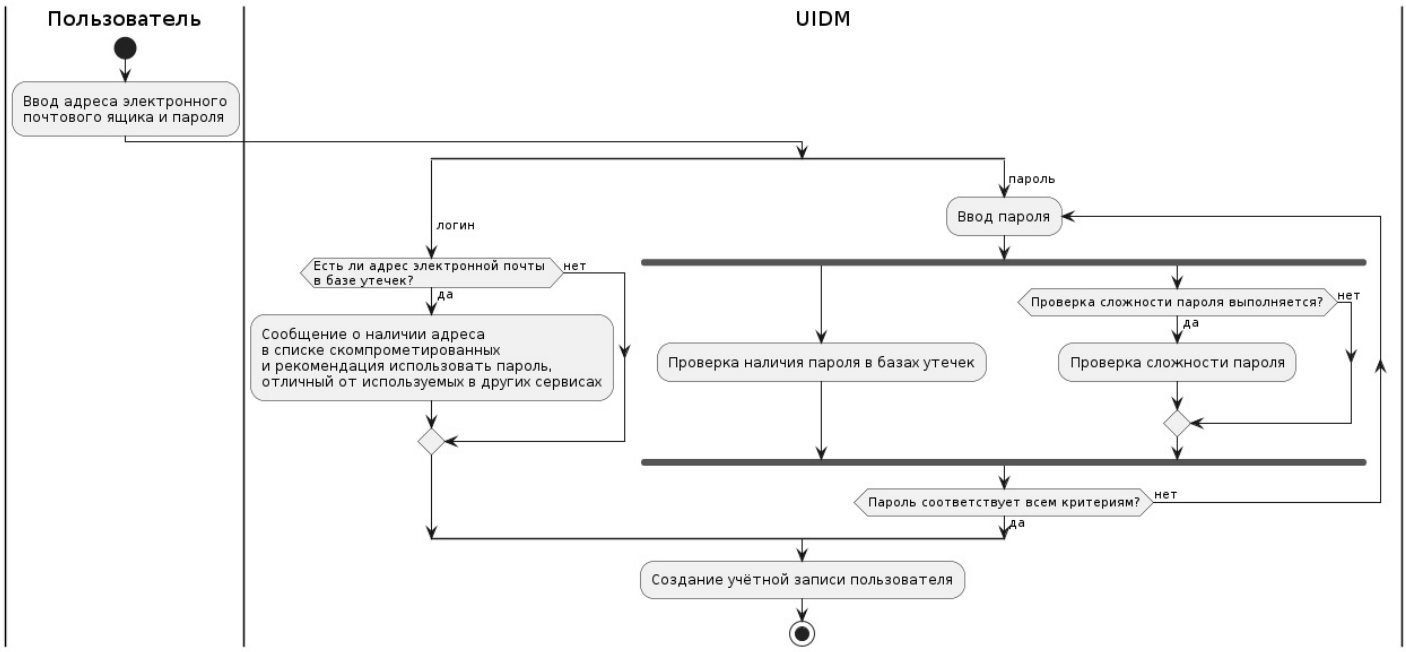
- проверку устанавливаемых или изменяемых паролей от учётных записей пользователей на минимальную сложность, обеспечивающую техническую затруднительность подбора такого пароля;
- проверку устанавливаемых или изменяемых паролей на предмет их наличия в словарях популярных или часто устанавливаемых паролей;
- проверку устанавливаемых или изменяемых паролей на предмет их наличия в известных списках скомпрометированных паролей.

Реакция UIDM на наличие пароля в справочнике простых или распространенных паролей зависит от сценария и настроек системы:

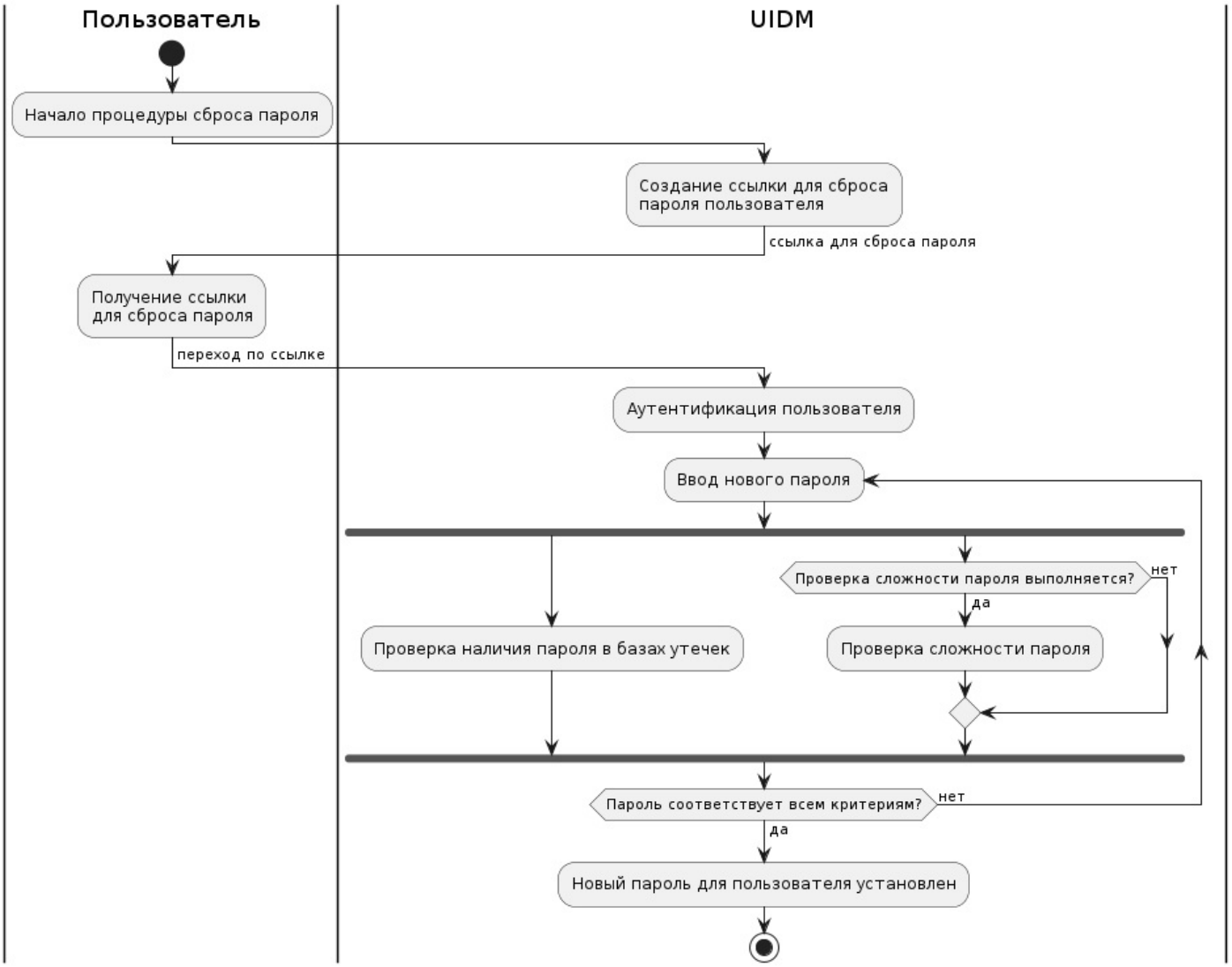
- в сценариях смены или установки нового пароля UIDM потребует от пользователя придумать новый пароль;
- в сценариях аутентификации UIDM порекомендует или потребует от пользователя сменить пароль.

Сценарии работы с использованием технических решений защиты

Сценарий регистрации нового пользователя



Сценарий сброса (изменения) пароля пользователя



Сценарий аутентификации пользователя