

Протокол тестирования биометрического решения liveness-проверки лица

«09» октября 2025 г.

Биометрическое решение liveness-проверки лица: SunSoft

Заявитель: ТОО «SunSoft»

Разработчик: SunSoft

Номер версии: 0.0.14

Номер сборки: 0.0.19

Дата проведения тестирования: с 29.09.2025 по 06.10.2025

Место проведения тестирования: АО «НПК» г.Алматы мкр. Коктем 3 д.21

ФИО работников, принимавших участие в тестировании:

Лазарев Александр Николаевич – главный системный аналитик отдела операционного сопровождения управления ЦОИД;

Цель тестирования:

- определить вероятность ложного допуска при совершении атак с использованием фотоизображений, масок, видеозаписей, deepfake технологий и их комбинации;
- определить вероятность ложного недопуска;
- определить пропускную способность биометрического решения liveness-проверки лица.

Перечень материальных и технических средств, использованных в ходе тестирования:

- Силиконовая маска мягкая на лицо, с вырезами глаз;
- Силиконовая маска жесткая на лицо, без вырезов;
- Силиконовая маска на всю голову, без вырезов;
- Фотоизображения лица, распечатанные на принтере Epson L805 (на матовой и глянцевой бумаге);
- ПО DeepFaceLive NVIDIA build 07.09.2023 с публичными моделями лиц;
- Системный блок:
 - CPU: Intel® Core i9 13900K;
 - RAM: 64 Gb;
 - SSD: 2 Tb;
 - GPU: nVidia RTX 4090
- Мобильный телефон Apple iPhone 14 Pro Max;
- Мобильный телефон Samsung Galaxy S22 Ultra;
- Планшет iPad 12.9 M2;
- Монитор Philips 28"

Для тестирования биометрического решения выделены следующие серверные вычислительные ресурсы:

CPU: Intel® Core i9 13900K;

RAM: 64 Gb;

SSD: 2 Tb;

GPU: nVidia RTX 4090

№	Вид тестирования		Описание процесса тестирования	Результат
1.	Общее тестирование функционала биометрического решения лайвнес-проверки лица			
1.1.	Тестирование корректной личностью	Имитация обычных условий	Проведено 500 сессий liveness	Успешно, BPCER менее 15%
2.	2D атаки (попытка авторизации злоумышленника вместо реального человека) биометрического решения лайвнес-проверки лица			
2.1.	Распечатанное фотоизображение лица	Использование фотоизображения лица (все лицо), распечатанного на матовой/ глянцевой бумаге	Попытка аутентификации с использованием фотоизображения лица, распечатанного на глянцевой и матовой фотобумаге	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
2.2.		Использование изогнутого фотоизображения лица (все лицо), распечатанного на матовой/глянцевой бумаге	Попытка аутентификации с использованием изогнутого фотоизображения лица, распечатанного на глянцевой и матовой фотобумаге	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
2.3.		Использование фотоизображения лица (с вырезом глаз), распечатанного на матовой/глянцевой бумаге, закрепленного на лице	Попытка аутентификации с использованием фотоизображения лица, распечатанного на матовой и глянцевой фотобумаге с вырезом в области глаз	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
2.4.		Использование фотоизображения лица (с вырезом области глаз и носа),	Попытка аутентификации с использованием фотоизображения	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА

		распечатанного на матовой/глянцевой бумаге, закрепленного на лице	лица, распечатанного на матовой и глянцевой фотобумаге с вырезом в области глаз и носа	
3.	Атака биометрического решения лайвнес-проверки лица с использованием видеозаписи или фотоизображения, демонстрируемого через устройства			
3.1.	Демонстрация фотоизображения	Демонстрация фотоизображения через мобильный телефон	Попытка аутентификации с использованием изображения лица демонстрируемого со смартфона на камеру (для демонстрации применялись iPhone 14 PRO MAX и Samsung Galaxy S22 Ultra)	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
3.2.		Демонстрация фотоизображения через планшет	Попытка аутентификации с использованием изображения демонстрируемого с планшета на камеру (для демонстрации применялся планшет iPad 12.9 M2)	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
3.3.		Демонстрация фотоизображения через монитор с матовым покрытием	Попытка аутентификации с использованием изображения демонстрируемого с монитора на камеру (применялся Philips 28")	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
4.	3D атаки (попытка авторизации вместо реального человека) биометрического решения лайвнес-проверки лица			
4.1.		Использование силиконовой маски (все лицо без вырезов)	Попытка аутентификации с использованием силиконовой маски лица (без вырезов)	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
4.2.		Использование силиконовой маски с вырезом в области глаз	Попытка аутентификации с использованием силиконовой маски	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА

			лица (с вырезом в области глаз)	
4.3.		Использование силиконовой маски (на всю голову)	Попытка аутентификации с использованием силиконовой маски на всю голову (без вырезов)	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
5.	Атака биометрического решения лайвнес-проверки лица, с использованием технологии deepfake			
5.1.		Атака биометрического решения liveness-проверки лица, с использованием технологии deepfake через мобильный телефон	Попытка аутентификации с использованием инструментов deepfacelive для подмены лица, изображение транслировалось со смартфона на камеру во время онлайн трансляции (для демонстрации применялись iPhone 14 PRO MAX и Samsung Galaxy S22 Ultra)	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
5.2.		Атака биометрического решения liveness-проверки лица, с использованием технологии deepfake через планшет	Попытка аутентификации с использованием инструментов deepfacelive для подмены лица, изображение транслировалось с планшета (для демонстрации применялся планшет iPad 12.9 M2) на камеру во время онлайн трансляции	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
5.3.		Атака биометрического решения liveness-проверки лица, с использованием технологии deepfake Через монитор с покрытием	Попытка аутентификации с использованием инструментов deepfacelive для подмены лица, изображение транслировалось с монитора на камеру (применялся Philips 28")	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА

5.4.		Атака биометрического решения liveness-проверки лица, с использованием технологии deepfake с подменой видеопотока	Попытка аутентификации с использованием deepfake и инструментов для осуществления подмены видеопотока	Проверка на живость не пройдена, результат - АТАКА УСПЕШНО ОТРАЖЕНА
5.5.		Атака биометрического решения liveness-проверки лица, с подменой видеопотока	Попытка аутентификации с использованием подмены видеопотока	Проверка на живость пройдена, результат - АТАКА НЕ ОТРАЖЕНА

Заключение:

Тестирование биометрического решения liveness-проверки лица SunSoft завершено успешно. Биометрическое решение liveness-проверки лица **SunSoft v.0.0.14 (фронт v.0.0.19)** **НЕ СООТВЕТСТВУЕТ** установленным требованиям.

Подписано:

Председатель Правления



Ж. Самаева

И.о. заместителя
Председателя Правления



Т. Попова

Начальник Управления
развития цифровых сервисов



А. Ермаханова

Главный системный аналитик
Отдела сопровождения Управления
развития цифровых сервисов



А. Лазарев