GIS DAYS 2021

«Риски от некорректного внедрения биометрии»

Николаев Данила Евгеньевич
Директор НП «Русское биометрическое общество», Председатель ТК 098 «Биометрия и биомониторинг» (Росстандарт)

Испытания и протоколы испытаний в области биометрии.
Алгоритмы и полнокомплектные биометрические системы

ГОСТ Р ИСО/МЭК 19795

Технологическое
(биометрический алгоритм)
(ГОСТ Р 58292–2018
(ИСО/МЭК 19795-2:2007)

Сценарное
(макет полнокомплектной биометрической системы)
(ГОСТ Р 58292–2018
(ИСО/МЭК 19795-2:2007)

Оперативное
(действующая полнокомплектная биометрическая система)
(ГОСТ Р ИСО/МЭК 19795-6–2015)

Испытания и протоколы испытаний в области биометрии. Обнаружение атаки на биометрическое предъявление

ГОСТ Р 58624.3

Метод (алгоритм) обнаружения атаки на биометрическое предъявление

Подсистема обнаружения атаки на биометрическое предъявление

Подсистема сбора биометрических данных

Возможные влияния ошибок распознавания на каждый уровень доверия по ISO/IEC 19989-2 Information security - Criteria and methodology for security evaluation of biometric systems - Part 2: Biometric recognition performance

Возможное влияние	Уровни доверия			
	Низкий	Средний	Высокий	Очень высокий
Вред, причиненный деловой репутации	Минимальный риск	Умеренный риск	Существенный риск	Высокий риск
Потеря финансовых ресурсов	Минимальный риск	Умеренный риск	Существенный риск	Высокий риск
Причинение вреда организации	N/A	Минимальный риск	Умеренный риск	Высокий риск
Несанкционированное разглашение конфиденциальной информации	N/A	Умеренный риск	Существенный риск	Высокий риск
Персональная безопасность	N/A	N/A	От минимального до умеренного риска	От существенного до высокого риска
Гражданские или уголовные нарушения	N/A	Минимальный риск	Умеренный риск	Высокий риск

Требования к минимальным значениям вероятности ложного доступа (ВЛД [FAR]) для проведения сценарных испытаний биометрических систем верификации по ISO/IEC 19989-2 Information security - Criteria and methodology for security evaluation of biometric systems - Part 2: Biometric recognition performance

- ВЛД (FAR) для очень высокого уровня доверия: не менее 0,000001% (10^{-8});
- ВЛД (FAR) для высокого уровня доверия: не менее 0,0001% (10^{-6});
- ВЛД (FAR) для среднего уровня доверия: не менее 0,01% (10^{-4});
- ВЛД (FAR) для минимального (базового) уровня доверия: не менее 1% (10^{-2}).

Примечание – *ВЛД = ВЛС*(1 - ВОСД)*,

где ВЛС – вероятность ложного совпадения, ВОСД – вероятность ошибки сбора данных

Текущая ситуация в нормативном-правовом регулировании биометрических технологий и возможные риски

Проект приказа «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации»

Текущая ситуация в нормативном-правовом регулировании биометрических технологий и возможные риски. Часть 1. Ошибки распознавания

Требования проекта приказа	Требования национальных и международных стандартов	Возможное влияние
ВЛС (для лица) – не более 0,0001; ВЛС (для голоса) – не более 0,1; Вероятности ложноположительной идентификации (ВЛПИ [для лица]) – не более 0,0001; ВЛПИ (для голоса) – не более 0,1	1. Необходимо также учитывать вероятность ложного несовпадения (ВЛНС) для биометрических систем верификации; 2. Необходимо также учитывать вероятности ложноотрицательной идентификации (ВЛОИ) для биометрических систем идентификации для нескольких порогов; 3. Необходимо учитывать ошибки первого и второго рода для различных сценариев использования; 4. Необходимо обеспечивать высокий и очень высокий уровни доверия	1. Вред, причиненный деловой репутации; 2. Потеря финансовых ресурсов; 3. Причинение вреда государству; 4. Причинение вреда организации; 5. Причинение вреда человеку

Текущая ситуация в нормативном-правовом регулировании биометрических технологий и возможные риски. Часть 2. Обнаружение атак

Требования проекта приказа	Требования национальных и международных стандартов	Возможное влияние
Вероятность ошибки классификации предъявления при атаке (ВОКПА) – не более 0,01 *(Примечание – Не определен перечень видов атак на биометрическое предъявление)*	- ВОКПА; - вероятность ошибки классификации подлинных биометрических предъявлений (ВОКПБП); - вероятность отсутствия ответа на предъявление артефакта (ВООПА); - вероятность отсутствия ответа на подлинное биометрическое предъявление (ВООПБП); - вероятность получения предъявления при атаке (ВППА); - вероятность совпадения предъявления при атаке самозванца (ВСПАС); - вероятность несовпадения предъявления при атаке укрывателя личности (ВНсПАУ); - вероятность идентификации предъявления при атаке самозванца (ВИПАС); - вероятность неидентификации предъявления при атаке укрывателя личности (ВНиПАУ); - длительность обработки.	1. Вред, причиненный деловой репутации; 2. Потеря финансовых ресурсов; 3. Причинение вреда государству; 4. Причинение вреда организации; 5. Причинение вреда человеку

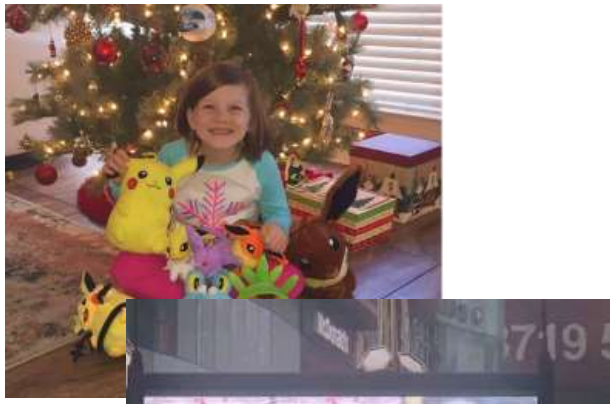
Текущая ситуация в нормативном-правовом регулировании биометрических технологий и возможные риски. Часть 3. Подтверждение соответствия

Требования проекта приказа	Требования национальных и международных стандартов	Возможное влияние
1. Требования к порядку проведению и видам испытаний (технологическое, сценарное, оперативное) не установлены; 2. Требования к базам данных и испытуемой группе не установлены	1. Устанавливают требования к порядку проведения технологических, сценарных и оперативных испытаний	1. Вред, причиненный деловой репутации; 2. Потеря финансовых ресурсов; 3. Причинение вреда государству; 4. Причинение вреда организации; 5. Причинение вреда человеку

Текущая ситуация в нормативном-правовом регулировании биометрических технологий и возможные риски. Часть 4. Не учтены все используемые биометрические модальности

Требования проекта приказа	Перечень используемых биометрических модальностей на территории РФ	Примечание
Распространяются только на: - изображение лица; - данные голоса, собранные текстонезависимым методом	- изображение отпечатка пальца; - изображение отпечатка ладони; - изображение радужной оболочки глаза; - изображение сосудистого русла; - данные голоса, собранные текстонезависимым методом; - данные походки; - данные силуэта	В следствие преднамеренного ограничения использования вышеприведенных параметров биометрических персональных данных физического лица в перспективе невозможно будет объединить биометрические база данных, в связи с использование как разных форматов обмена, т.к. и разных требований к сбору данных

Теоретические примеры потери финансовых ресурсов и как следствие причинение вреда деловой репутации из-за атаки, связанной с принуждением человека (включая бессознательное состояние)



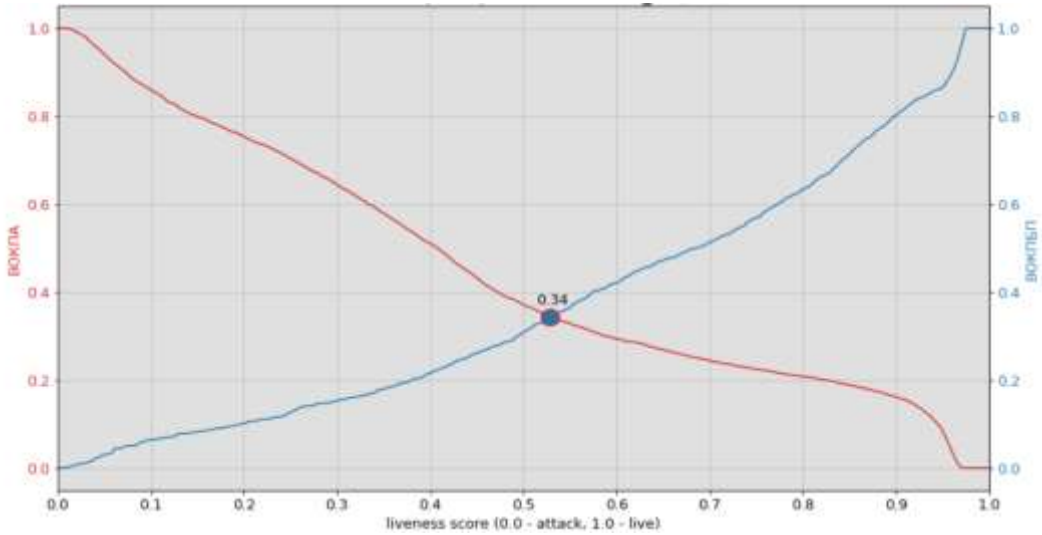
Реальные примеры потери финансовых ресурсов

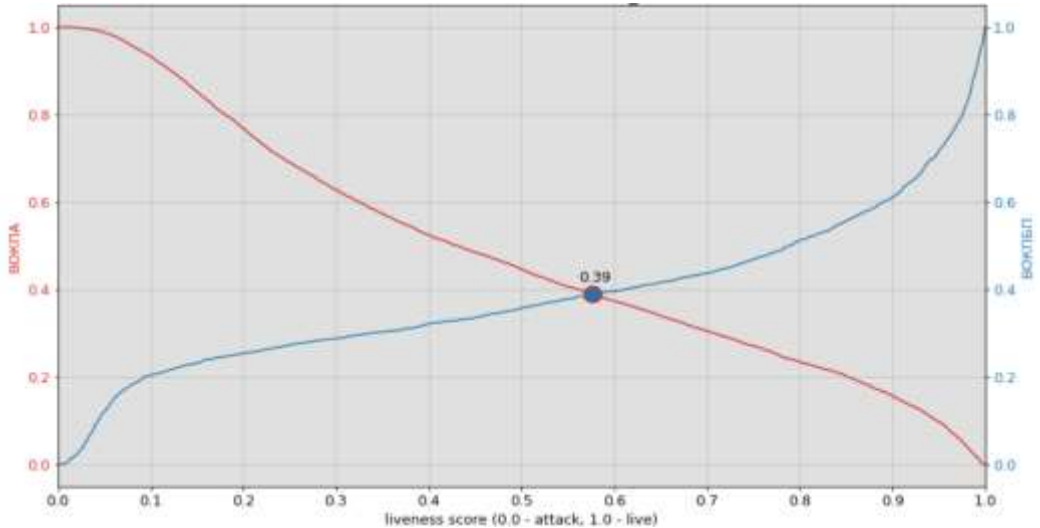
Девочка воспользовалась отпечатком пальца *спящей* *мамы*, чтобы заказать в интернете подарки (13 покемонов) на $250.

Система, развернутая китайским правительством для идентификации пешеходов, использующая распознавание лиц в режиме реального времени, ошибочно определила знаменитость как преступника после сканирования лица из рекламы на проходящем автобусе.


Tom Cruise

Теория и практика. Реальные значения метрик на инфраструктуре Заказчика





GIS DAYS

РБО

Спасибо за внимание!

www.rusbiometrics.com