

Биометрия в информационных системах. Можно ли без этого выжить?

Форум All-over-IP 2017, 24 ноября 2017 г.

Дмитрий Пшеннов, Fujitsu Россия и СНГ

Об идентичности

- Каждое существо уникально и имеет свою индивидуальную идентичность
 - Все начинается тогда, когда родители дают нам идентичность при рождении
 - Наш первый документ идентичности – свидетельство о рождении
 - Позже мы получаем свой первый паспорт
 - А еще позже идентифицируем себя вклеиванием фотографий в него
 - Но также мы используем другие документы и инструменты в течение жизни:
 - Водительское удостоверение, страховое свидетельство, платежные карты, карты лояльности, имя входа в компьютер, e-mail, экаунты в социальных сетях, банковские счета, экаунты в онлайн магазинах, ИНН и т.д., и т.п.



Как защитить свою идентичность?

- Паспорта и идентификационные карты, использующие возможности биометрии
- Ежедневное использование компьютеров, планшетов и смартфонов для входа в Интернет, выполнения операций и действий, требующих идентификации
- Мы используем PINы, жетоны, смарткарты, пароли, образы для того, чтобы обезопасить свое имя, представляющее нашу идентичность
- Мы пытаемся обеспечить большую безопасность использованием многофакторности, но...



Госсектор

Персональная
идентификация



Идентификация
гражданина



Полиция/Пожарная
охрана (идентификация
пользователя)



Контроль доступа



Контроль доступа



Контроль присутствия



Полицейский портал

Доступ к
истории болезни



Идентификация
пациента



Контроль доступа
(склад)



Контроль доступа
(палаты новорожденных)



EMR-доступ

サーバ室の入退室管理



病歴室の入退院管理

Доступ в серверные



Идентификация пациента
перед операцией

Образование

Идентификация
присутствия



Идентификация
студента



Кафе, столовая
(безналичный расчет)



Библиотека
(бескарточная
идентификация)



Подтверждение карты
студента



Бескарточная система
предоставления
учебников



Доступ в детские
помещения

Контроль присутствия



Регистрация



Контроль доступа POS-терминалы и SCO
(идентификация оператора)



Защита информации



Физический контроль
доступа на склад



Контроль рабочего
времени

Производство

Контроль доступа к
производству



Контроль
присутствия



CAD (Идентификация
оператора)



Контроль
доступа



Контроль времени и
присутствия



Контроль доступа к дата-
центру



Контроль доступа к
производству молока

Финансовый сектор

Банкоматы

(Снятие и перевод денег, в т.ч. пенсий и бескарточный)



Банковский терминал (VIP идентификация)



Back Office (Операторы)



Бескарточные цифровые киоски



Контроль доступа (касса, кабинет)



Биометрическая смарт-карта для клиентов



Доступ к дата-центру



Защита информации

Цена безопасности

	Секретный вопрос	СМС / 1-разовый пароль	Карты / токены	Однофакторная биометрия	Многофакторная биометрия
Трудозатраты на IT	\$	\$	\$	\$	\$
Удобство регистрации	Сложно	Сложно	Сложно	Просто	Просто
Удобство пользования	Сложно	Сложно	Сложно	Просто	Просто
Риск утери / кражи	Переменно	Да	Да	Нет	Нет
Уровень безопасности	*	***	***	****	*****

#1 ВЕКТОР АТАКИ -
СЛАБЫЕ ИЛИ СКОМПРОМЕТИРОВАННЫЕ ПАРОЛИ

81% НЕПРАВОМЕРНОГО ДОСТУПА К ДАННЫМ – ИЗ-ЗА
СЛАБЫХ, «ПО УМОЛЧАНИЮ» ИЛИ УКРАДЕННЫХ ПАРОЛЕЙ

СРЕДНЕГОДОВЫЕ ПОТЕРИ ИЗ-ЗА ЭТОГО США - ОКОЛО
\$7МЛРД

ПОТЕРИ ИЗ-ЗА КИБЕРПРЕСТУПЛЕНИЙ ВЫРАСТУТ К 2019 Г.
ДО \$2 ТРЛН***

* [2017 Data Breach Industry Forecast](#)

** [2016 Ponemon Cost of Data Breach Study](#)

*** [Cyber Crime Costs Projected to Reach \\$2 Trillion by 2016](#)

Потери Вашего бизнеса

**50% организаций пострадали
от потерь данных в 2016**

29%

Потерь
оборота

22%

Потерь
клиентов

23%

Потерь
нового
бизнеса

\$7млн

Средние
потери на
компанию

Необходимость биометрической защиты данных



Определите критичность действий/программных приложений:

- Какова вероятность потери/искажения/несанкционированного использования данных
- Сколько стоит страхование данных
- Какими организационными способами можно решить задачу защиты данных, сколько это будет стоить
- Каков уровень защиты, который необходимо реализовать

Постройте целевой функционал защиты данных:

- Цена потери
- Вероятность
- Затраты
- Возможность контроля
- Потребные ресурсы
- Возможность модификации

Выберите правильный способ биометрической защиты данных

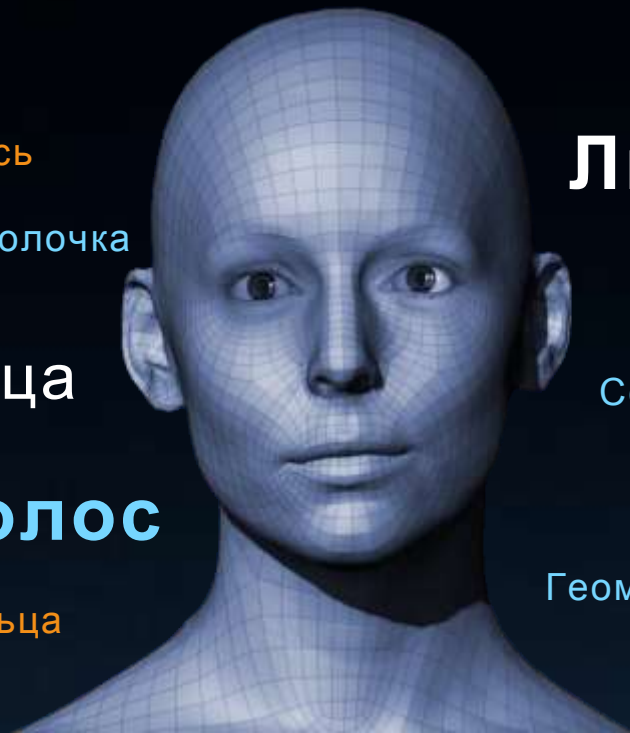
- Зависит от уровня необходимой защиты
- Зависит от требований законодательства
- Зависит от целевой аудитории
- Зависит от имеющихся ресурсов
- Зависит от возможностей аутсорсинга
- Зависит от наличия решения

Необходимость биометрической аутентификации **FUJITSU**



Многофакторная биометрия

Использование нескольких способов биометрии для
улучшенного обеспечения идентичности



Подпись

Радужная оболочка

Отпечаток пальца

Голос

Вены пальца

Лицо

Поведение

Сетчатка

Вены ладони

Геометрия руки

И более...

Идентифицировать пользователя, а не устройство

Что у Вас есть:

Устройства:
Смартфон, планшет,
компьютер и т.п.

Что Вы знаете:

Имя входа и пароль:
Аутентификация по знаниям

Кто Вы:

Вы сами - пароль:
Мультфакторная биометрия

Сравнение методов биометрии

	Вены ладони	Отпечаток пальца	Лицо	Радужная оболочка глаза
Точность аутентификации	Отлично	Хорошо	Удовлетворительно	Хорошо
Количество ошибок	Очень мало	Много	Очень мало	Средне
Скорость аутентификации	Быстро	Медленно	Очень быстро	Быстро
Уязвимость к подлогу	Высокая	Низкая	Низкая	Высокая
Прочность сенсора	Очень хорошая	Удовлетворительная	Очень хорошая	Очень хорошая
Чувствительность к внешним факторам	Очень низкая	Очень высокая	Очень высокая	Очень высокая

Законы, регулирующие защиту данных и безопасность данных:

- Приобретение, хранение и обработка биометрических данных разрешается только в том случае, если имеется правовая основа или добровольное и информированное согласие лица
- Биометрические данные могут использоваться только для той цели, для которой они были собраны, например, для контроля доступа

Требования к соглашению о защите данных:

- Используйте не исходные данные, а производные (темплейты)
- Предоставьте выбор процедур
- **Использование локального хранения данных** – под контролем пользователя, н-р SmartCard)
- Защита биометрических данных от несанкционированного доступа
- Использование криптозащиты
- Прозрачность процедур и механизмов защиты

Заключение:

Проблемы защиты данных не применяются, если

- Центральный носитель данных не используется и пользователи сами управляют хранением своих биометрических характеристик
- Выполняется требование ЕС о двухфакторной аутентификации для платежных процессов

Низкий уровень защиты:

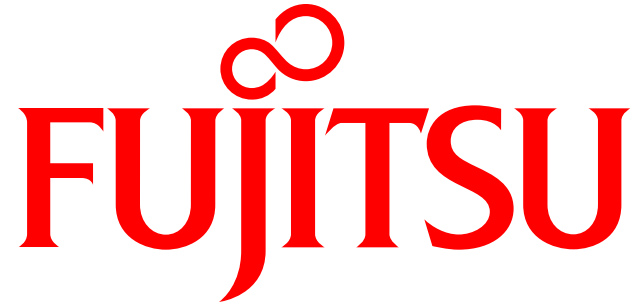
- Персональное использование доступа
- Трудоемкость подбора
- Ограниченное число имеющих доступ
- Редкое в течение дня использование
- Использование локальной верификации
- Возможность использования авторизованных устройств

Средний уровень защиты:

- Массовое использование доступа
- Низкая вероятность ошибки
- Частое использование устройства
- Использование локальной верификации
- Возможность использования вероятностных моделей

Высокий уровень защиты:

- Массовое использование доступа
- Высокая вероятность ошибки
- Частое использование устройства
- Использование глобальной верификации
- Требование абсолютной надежности



shaping tomorrow with you