Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

# Методы оценки доверия к результатам первичной идентификации

Алексей Сабанов, к.т.н., доцент МГТУ им. Н.Э. Баумана,
Заместитель генерального директора ЗАО «Аладдин Р.Д.»
Эксперт ISO/JTC1/SC27/WG5, член ТК362, ТК122, академик МАС

# Введение

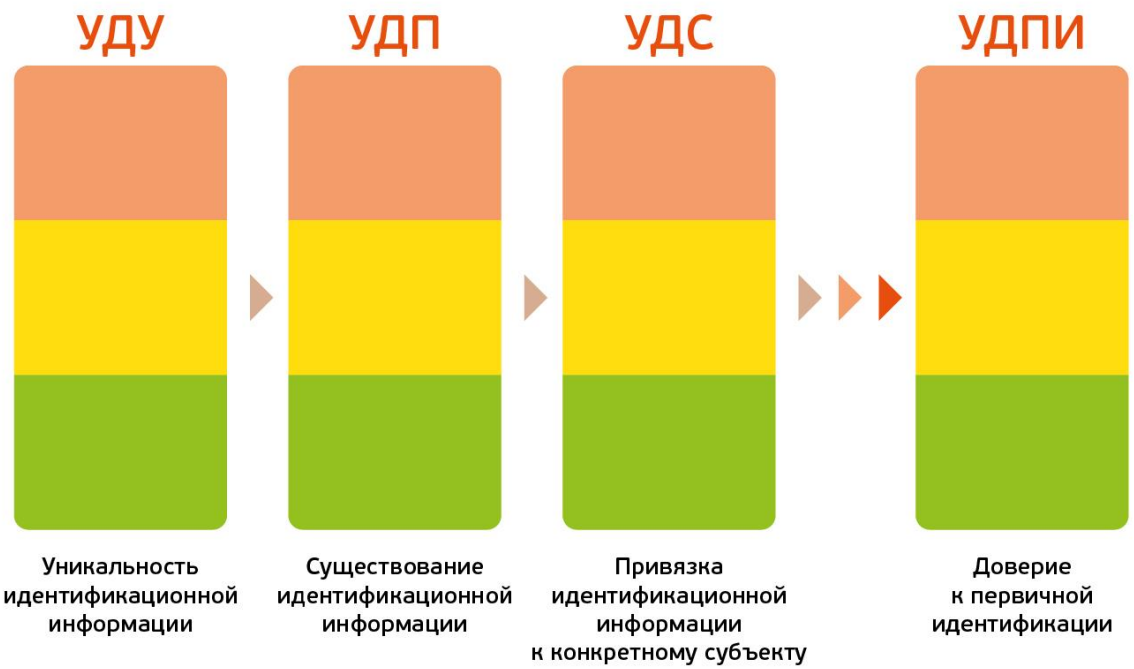
- Не надо путать идентификацию в целях идентификации (СКУД, реестры населения) и идентификацию для последующего регулярно повторяющегося процесса вторичной идентификации, аутентификации для предоставления доступа.
- Также сильно отличаются обычный и удаленный доступ. Требования к безопасности в последнем случае значительно выше.
- В данном докладе рассматривается первичная идентификация для использования ее результатов в целях предоставления доступа.

# Процесс первичной идентификации

# Характеристики доверия к результату первичной идентификации

| Первичная регистрация субъекта (объекта) доступа | | | Допущения, определяемые правилами управления доступом | Уверенность в том, что субъект (объект) доступа действительно соответствует заявленным идентификационным данным | Уровень доверия к результатам первичной идентификации | Возможность регистрации субъекта (объекта) доступа |
|---|---|---|---|---|---|---|
| Уникальность идентификационной информации | Подтверждение идентификационных данных | | | | | |
| | Существование идентификационных данных | Привязка идентификационных данных | | | | |
| Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации | | | Необходимо подтверждение идентификационных данных | Нет никакой уверенности | Доверие к идентификационным данным отсутствует | Отказ в регистрации субъекта (объекта) доступа |
| Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации | | | Отсутствует необходимость подтверждения идентификационных данных | Нет никакой уверенности | Доверие к идентификационным данным отсутствует | Регистрация субъекта (объекта) доступа как «анонима» |
| Уникальность обеспечивается | Существование идентификационных данных не проверяется | Привязка идентификационных данных не проверяется | Необходимо подтверждение идентификационных данных | Некоторая уверенность | Низкий уровень доверия к идентификационным данным | Регистрация субъекта (объекта) доступа |
| Уникальность обеспечивается | Существование идентификационных атрибутов и достоверность их значений в подтверждающих свидетельствах | Привязка идентификационных данных с использованием одного фактора | Необходимо подтверждение идентификационных данных | Умеренная уверенность | Средний уровень доверия к идентификационным данным | Регистрация субъекта (объекта) доступа |
| Уникальность обеспечивается | Существование идентификационных атрибутов и достоверность их значений в официальных свидетельствах | Привязка идентификационных данных с использованием не менее двух факторов | Необходимо подтверждение идентификационных данных | Высокая уверенность | Высокий уровень доверия к идентификационным данным | Регистрация субъекта (объекта) доступа |

# Формирование уровней доверия к результатам первичной идентификации

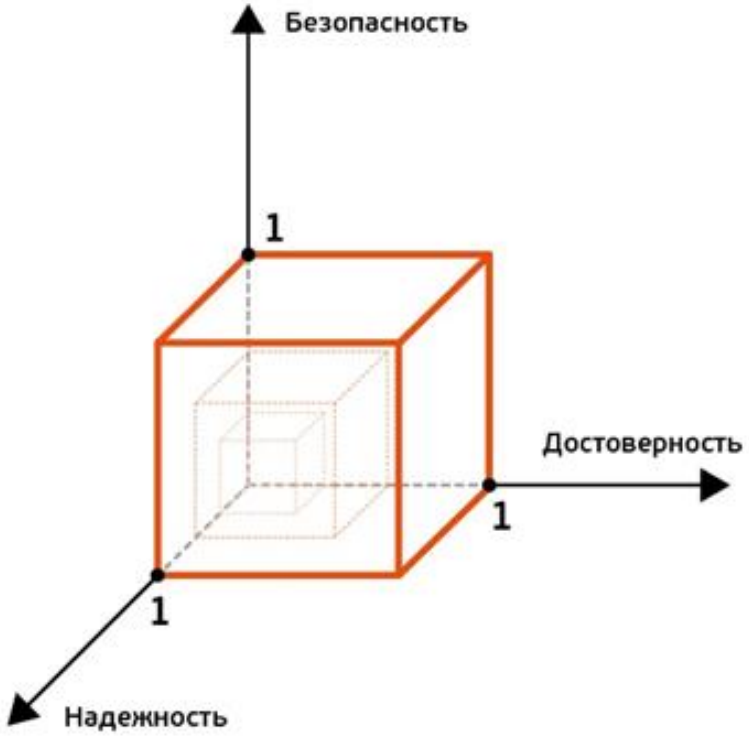


# Критерии доверия

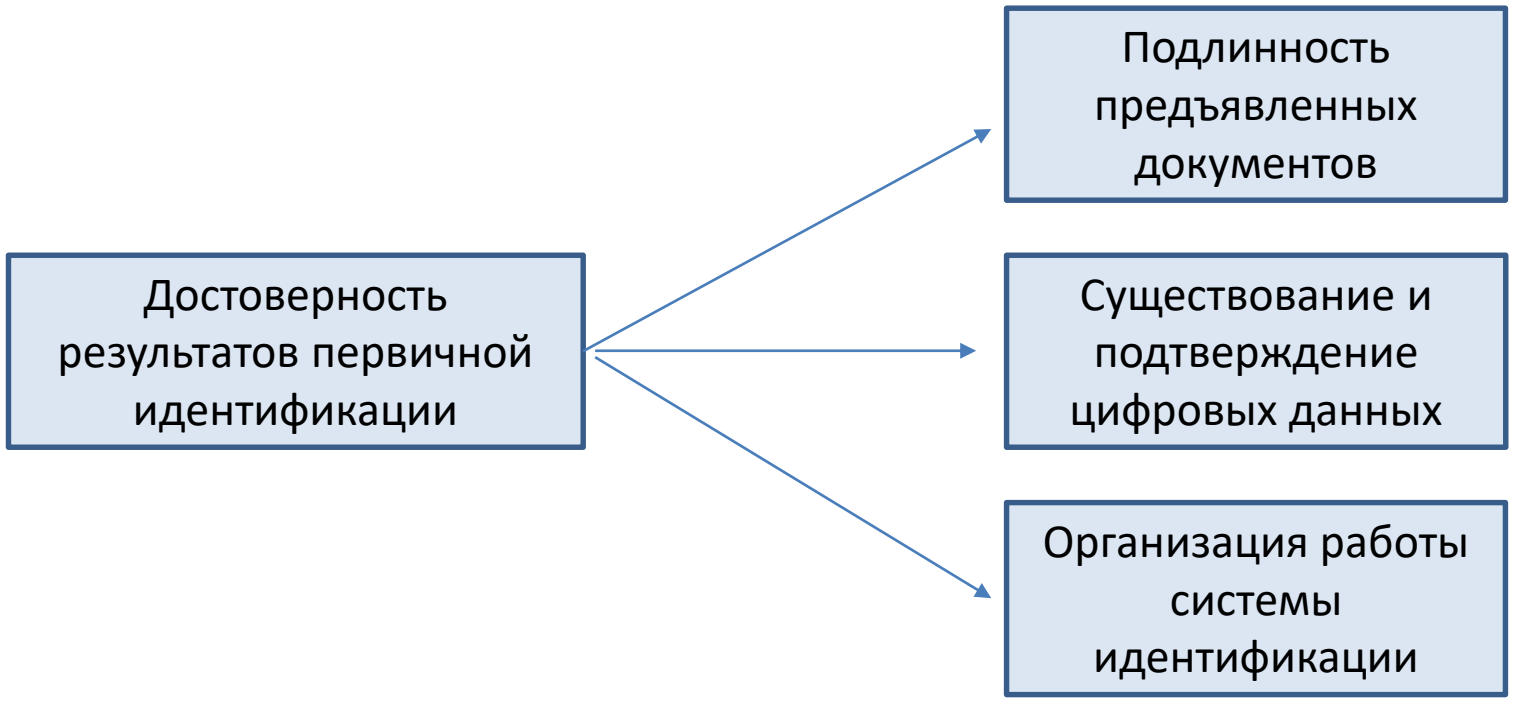
1. **достоверность** (полнота, точность, аутентичность и степень связанности с заявителем) результатов;
2. функциональная **надежность** работы системы идентификации;
3. выполнение в процессе первичной идентификации требований **информационной безопасности**, в том числе в отношении персональных идентификационных данных субъектов доступа;

# Задача оценки доверия

поиск решений $\psi\ [\varphi_Б(t),\ \varphi_Д(t),\ \varphi_Н(t)]$



# Оценка достоверности результатов



# Оценки достоверности цифровой идентификации. Работа системы идентификации

Достоверность информации *D (t) = D*± ΔD, где ΔD – доверительный интервал.*

Для грубых оценок достоверности рассмотрим модель на основе МКА, заключающуюся в том, что проверку каждого предъявленного идентификационного атрибута будем считать независимо (по надежности) работающим прибором.

Надёжность работы системы определяется соотношением

$$H_c = 1 - \prod_{i=1}^{N} (1 - H_i) \qquad (5)$$

где $H_i$ – надёжность каждого элемента системы,

Достоверность идентификации определяется *

$$P_c(t) = 1 - q_1(t) \cdot q_2(t) \cdot \ldots \cdot q_n(t) = 1 - \prod_{i=1}^{n} (1 - p_i(t)) \qquad (6)$$

где $q_i$ - вероятность ошибки работы подсистемы при сравнении i-го идентификационного атрибута, $p_i\ (t)$ – вероятность отсутствия ошибки.

Утверждение. В больших системах с числом пользователей К (современные ИС уже имеют количество пользователей до значения $К=10^6$-$10^8$) для выполнения основной функции идентификации - уникальности и различимости каждого субъекта из общего количества пользователей необходимо достигать значение достоверности идентификации не ниже

$D = 1 - 1/(K+1)$.

*) М. Ю. Монахов, Ю. М. Монахов, Д. А. Полянский, И. И. Семенова. Модели обеспечения достоверности и доступности информации в информационно-телекоммуникационных системах : монография / М. Ю. Монахов [и др.] ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2015. – 208 с.

# Как делаются оценки вероятности ошибок?

Вероятности ошибок человека-оператора(технолога)

| **Вид ошибки**<br>Ошибки считывания информации: | **Вероятность ошибки** [1] |
|---|---|
| • одинарного алфавитно-цифрового знака | $2 \cdot 10^{-4}$ |
| • пятибуквенного слова при хорошем различении | $3 \cdot 10^{-4}$ |
| • проверочного списка или цифрового показания | $1 \cdot 10^{-3}$ |
| • десятизначного числа | $6 \cdot 10^{-3}$ |
| Неисполнение отдельного требования при наличии памятки (инструкции) на рабочем месте | $1 \cdot 10^{-3}$ |
| То же при отсутствии памятки и содержании в инструкции<br>- до 10 требований<br>- более 10 требований | <br>$3 \cdot 10^{-3}$<br>$1 \cdot 10^{-2}$ |
| Записи числовой информации (более 3 цифр) | $10^{-3}$ на одну цифру |

Известно, что ошибки операторов наиболее часто встречаются в ИС и составляют от 15% до 30% от общего числа ошибок функционирования информационных систем.

1. Шубинский И.Б. Функциональная надёжность информационных систем. Методы анализа/ И.Б.Шубинский - Ульяновск: областная типография «Печатный двор», 2012. – 296с.

# Оценки ошибок при передаче

Типовое сообщение в системе идентификации и аутентификации, полученное от претендента на идентификацию представляет собой $n$ последовательно передаваемых бит информации.

Предполагается, что канал биномиальный, т.е. вероятность $k$ ошибок на длине сообщения $n$ определяется как $P(k,n) = C_n^k p^k (1-p)^{n-k}$

где $p$ – вероятность ошибки на бит; $k$ - длина блока информационных бит, $n$- длина всего сообщения в битах, где $N$ – количество байт данных сообщения; количество контрольных бит – 16 (код CRC).

При приеме сообщения должен быть реализован информационный процесс, включающий 1. проверка правильности типа пакета; 2. определение адреса отправителя; 3. определение адреса получателя; 4. проверка длины сообщения;5. проверка правильности контрольных бит (проверка контрольной суммы). Эти процессы в соответствии с уровнями иерархии упорядочиваются таким образом:1-5; 2-4; 3-3; 4-2; 5-1.

При приеме сообщения процессы выполняются в обратном порядке: вначале выполняется процесс 5, затем 4, затем 3, затем 2, затем 1.

Вероятность ошибки (трансформации) всего сообщения в предположении, что вероятность $1 - (1 - p)^{16} \approx 1$, можно оценить: $G_N = \prod_{i=1}^{4} G_i \approx [1 - \frac{1}{2^{16}} \sum_{i=r+1}^{n} C_n^i p^i (1-p)^{n-i}] \cdot \prod_{j=1}^{4} \frac{2^{16} + 1 - K_j}{2^{16}}$

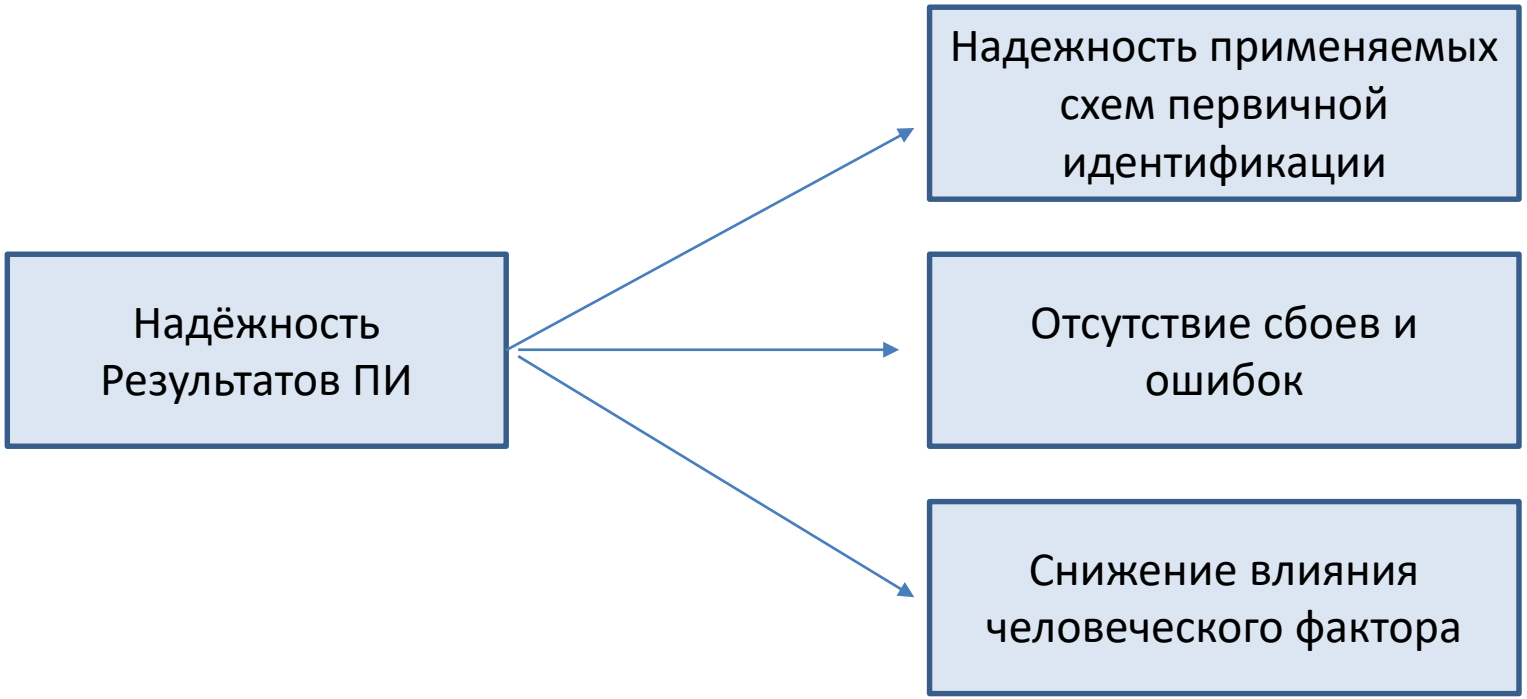
# Оценка безопасности и уровни доверия к результатам первичной идентификации

| | *Цели* | *Задачи* | *I уровень доверия* | *II уровень доверия* | *III уровень доверия* |
|---|---|---|---|---|---|
| **Доступность** | Гарантии обработки запросов на аутентификацию | Отказоустойчивость СИА, обеспечение необходимой производительности | Допустима очередь заявок | Ограничение длины очереди | Гарантированное обслуживание с ограничением длины очереди |
| | Разделение доступа | Идентификация пользователя Аутентификация пользователя | Вероятность ошибки идентификации $10^{-4}$-$10^{-2}$ | Вероятность ошибки идентификации $10^{-4}$-$10^{-6}$ | Вероятность ошибки идентификации $10^{-6}$-$10^{-8}$ |
| | Управление доступом | Заведение новой учетной записи (УЗ), приостановка доступа, отзыв, изменение прав доступа, удаление УЗ | Соблюдение регламента | Неквалифицированный сертификат доступа | Квалифицированный сертификат доступа |
| | Персонификация доступа | Жесткая привязка ИД и АИ к конкретному пользователю | Уникальный профиль доступа | Неквалифицированный сертификат доступа или OTP | Квалифицированный сертификат доступа |
| **Конфиденциальность** | Конфиденциальность учетных записей | Защита БДУЗ от НСД | Защита от НСД орг. мерами, хэширование учетных записей | Усиленная защита от НСД | Qualified Signature Creation Device |
| | Конфиденциальность АИ пользователя | Запрет экспорта ключей, орг. и тех. меры защиты АИ от НСД | Пользователь несет ответственность за сохранение пароля в тайне | Security Signature Creation Device или SSO+Смарт-карта | Шифрование учетных записей, хэширование ИД и АИ |
| | Конфиденциальность ПДн пользователя | Обеспечение защиты ПДн пользователя | Защита БДУЗ от НСД | Выполнение регламента по защите БДУЗ от НСД | Шифрование ПДн в БДУЗ |
| **Целостность** | Целостность системного и прикладного ПО ПсИА | Обеспечение целостности ПО ПсИА и клиенского ПО | Программные средства контроля целостности | Комбинированные средства контроля целостности | Аппаратные средства хранения контрольных сумм и ключей |
| | Целостность учетных записей в БДУЗ | Обеспечение целостности учетных записей пользователей в БД сервера аутентификации | Хэширование учетных записей | Хэширование учетных записей | Хэширование учетных записей, электронная подпись |
| | Целостность АИ пользователя в БДУЗ и у владельца АИ | Обеспечение целостности АИ пользователя при генерации, хранении, предъявлении и передаче | Хранение АИ в БДУЗ только в хэшированном виде | Хранение АИ в БДУЗ только в хэшированном виде и/или открытые ключи пользователей | БДУЗ содержит только открытые ключи пользователей |

**Треб. ФН**

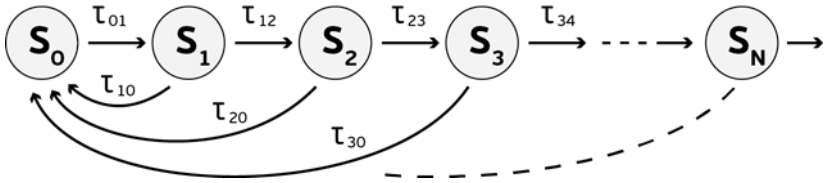
**Требования ИБ к системе идентификации и аутентификации**

# Оценка надёжности результатов



# Функциональная надежность

# Оценка надежности работы схемы последовательных проверок




$S_0$ – состояние системы: система готова.

$S_1$ – первый идентификатор предъявлен, система провела его проверку;

$S_2$ – второй идентификатор предъявлен, система провела его проверку;

$S_3$ – идентификация успешно пройдена, система передала управление системе аутентификации;

$S_4$ – подсистема аутентификации приняла идентификационные данные пользователя.

$\tau_{01}$ – претендент предъявляет системе первый идентификатор;

$\tau_{12}$ – претендент предъявляет системе второй идентификатор;

$\tau_{23}$ – претендент успешно прошёл идентификацию;

$\tau_{10}$ – подсистема идентификации возвращает процесс в начало (состояние $S_0$) из-за несовпадения первого идентификатора;

$\tau_{20}$ – подсистема идентификации возвращает процесс в начало из-за несовпадения второго идентификатора;

$\tau_{30}$ – подсистема идентификации возвращает процесс в начало из-за несовпадения третьего идентификатора;

$\tau_{34}$ – подсистема идентификации передаёт данные претендента в подсистему аутентификации;

$P_0(t)$ – вероятность того, что в момент времени $t$ система находится в состоянии $S_0$;

$P_i\ (t)$ – вероятность пребывания системы в состояниях $S_i$.

# Оценка надежности ПИ: аналитическое решение

Тогда уравнения Колмогорова для рассматриваемой системы могут быть представлены в виде:

$$\frac{dP_0(t)}{dt} = -\tau_{01}P_0(t) + \tau_{10}P_1(t) + \tau_{20}P_2(t) + \tau_{30}P_3(t);$$

$$\frac{dP_1(t)}{dt} = -\tau_{12}P_1(t) - \tau_{10}P_1(t) + \tau_{01}P_0(t) + \tau_{30}P_3(t) = -P_1(t)(\tau_{10} + \tau_{12}) + \tau_{01}P_0(t);$$

$$\frac{dP_2(t)}{dt} = -\tau_{23}P_2(t) - \tau_{20}P_2(t) + \tau_{12}P_1(t) = -P_2(t)(\tau_{20} + \tau_{23}) + \tau_{12}P_1(t);$$

$$\frac{dP_3(t)}{dt} = -\tau_{34}P_3(t) - \tau_{30}P_3(t) + \tau_{23}P_2(t) = -P_3(t)(\tau_{30} + \tau_{34}) + \tau_{23}P_2(t);$$

$$P_0(t) + P_1(t) + P_2(t) + P_3(t) = 1,$$

так как для любых t должно выполняться равенство $\sum_{i=1}^{3} P_i(t) = 1$.

Примем начальные условия в виде

$$P_0(0) = 1;$$

$$P_1(0) = P_2(0) = P_3(0) = 0.$$

$$P_j = \frac{\tau_{ij}}{\tau_{ji} + \tau_{jk}} P_i$$

# Надежность параллельной схемы проверки идентификационных атрибутов

Из определения системы, состоящей из параллельно соединённых элементов, условием безотказной работы системы $P_c$ является безотказная работа хотя бы одного элемента $P_i$, i= 1,n.

Если считать отказы элементов независимыми, то на основании теоремы умножения вероятностей вероятность безотказной работы системы определяется следующим выражением:

$$P_c(t) = 1 - q_1(t) \cdot q_2(t) \cdot \ldots \cdot q_n(t) = 1 - \prod_{i=1}^{n} (1 - p_i(t)) \quad (6)$$

где $P_c(t)$ – вероятность безотказности работы системы, $q_i(t)$ – вероятность отказа работы i-го элемента $p_i(t)$ – вероятность безотказной работы i-го элемента.

Принимая, что вероятность безотказной работы каждого элемента $p_i(t)$ на отрезке времени $(t_1,t_2)$ подчиняется зависимости

$$p_i(t_1, t_2) = e^{-\int_{t_1}^{t_2} \lambda(t)dt} \quad (7)$$

где λ(t) – интенсивность отказа элемента. С учетом (7) выражение (6) примет вид

$$P_c(t) = 1 - \prod_{i=1}^{n} (1 - e^{\int_0^t \lambda_i(t)dt}) \quad (8)$$

# Аналитическое решение

Следовательно, если надежность каждого элемента подчиняется экспоненциальному закону, то надежность системы этому закону не подчиняется.

$$P_c(t) = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda t})$$

Для случая (9) легко вычисляется средняя наработка до отказа систем

$$t_{ср.с} = \int_0^\infty P_c(t)dt = \int_0^\infty \left[1 - (1 - e^{-\lambda t})^n\right]dt$$

При замене переменных

$$1 - e^{-\lambda t} = x;$$

$$t = \frac{1}{\lambda}\ln\frac{1}{1-x};$$

$$dt = \frac{dx}{\lambda(1-x)};$$

$$t = 0; x = 0;$$

$$t = \infty; x = 1;$$

Получим $t_{ср.с} = \frac{1}{\lambda}\int_0^\infty \frac{1-x^n}{1-x}dx = \frac{1}{\lambda}\int_0^1 (1 + x + \ldots + x^{n-1})dx = \frac{1}{\lambda}(1 + \frac{1}{2} + \ldots + \frac{1}{n})$ при больших n $t_{ср.с} \approx \frac{1}{\lambda}(\ln n + C)$, C=0,577

# Применение биометрии в идентификации

- Биометрия используется только в дополнение к другим идентификационным атрибутам (паспорт, СНИЛС, ИНН,...). «Биометрическое распознавание не может использоваться изолированно или вместо верификации других идентифицирующих атрибутов» - ISO/IEC 29003, раздел B4.
- Биометрия может использоваться для предотвращения дублирования записи, связанной с конкретным субъектом, в реестре (сравнение биометрического образца субъекта с другими биометрическими образцами. Собранная биометрическая информация должна быть достаточной и эффективной для исключения дублирования идентификационных данных - ISO/IEC 29003 29003, п.4.8 )
- Противодействие попыткам множественной регистрации.
- Подтверждение идентификационных данных
- Неотказуемость от регистрации нового пользователя ИС
- *Установление привязки идентификационной информации к конкретной личности*: привязка устанавливается путем сопоставления биологической или поведенческой характеристики, наблюдаемой подтверждающей стороной, с эталонной биометрической информацией, которая, как известно, соответствует субъекту - ISO/IEC 29003, разд. 5.5

# Причины: NIST SP 800-63B, June 2017

- биометрический коэффициент ложного совпадения (FRR) не обеспечивает уверенность в результатах идентификации пользователя. Кроме того, коэффициент ложного совпадения не учитывает атаки спуфинга;
- биометрическое сравнение вероятностно, а другие факторы аутентификации являются детерминированными;
- схемы защиты биометрических образцов пока не обеспечивают уровень хранения биометрических образцов, сопоставимых с другими факторами аутентификации (например, сертификаты доступа инфраструктуры открытых ключей). Доступность биометрических решений ограничена, и стандарты тестирования этих методов находятся в стадии разработки;
- биометрические характеристики не являются секретами и не способны генерировать секрет. Их можно получить онлайновым образом или тайно сфотографировав легального пользователя на камеру телефона или сняв скрытно отпечатки пальцев или получив с изображений с высоким разрешением (например, узор радужной оболочки глаза). Хотя технологии обнаружения атак путем представления (PAD) (например, детекторы присутствия) могут снижать риск таких видов атак, требуется дополнительное доверие к датчику или биометрической обработке для обеспечения уверенности в том, что обнаружение атак PAD защищает легального пользователя.

# Следствие: ограничения на применение биометрии

- Биометрические данные ДОЛЖНЫ использоваться только как часть многофакторной аутентификации с физическим аутентификатором (*фактор владения, например, смарт-картой*).
- ДОЛЖЕН быть установлен аутентифицированный защищенный канал между датчиком (или конечной точкой, содержащей датчик, которая является устойчивой к замене датчика) и проверяющей стороной, и датчик или конечная точка ДОЛЖНЫ аутентифицироваться до сбора биометрического образца у заявителя.
- Биометрическая система ДОЛЖНА действовать с коэффициентом ложного совпадения [ISO/IEC 2382-37] 1:1000 или более хорошим. Этот коэффициент ложного совпадения ДОЛЖЕН быть достигнут в условиях сообразной атаки (т.е. попытки самозванца с нулевыми усилиями), как определено в [ISO/IEC 30107-1].

# Вопросы

# Контактная информация

Электронная почта:
asabanov@mail.ru

Телефон:
+7-985-924-52-09

Сайт:
www. Aladdin-rd.ru