Трошков А.М.
кандидат технических наук, доцент
Ставропольский государственный аграрный университет
Кондрашов А.В.
кандидат технических наук
Ставропольский государственный аграрный университет
Горденко Д.В.
кандидат технических наук, доцент
Ставропольский государственный аграрный университет

ЖИВУЧЕСТЬ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ – БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ УПРАВЛЕНИЕМ ДОПУСКА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

В условиях вхождения России в ВТО, глобализации общества информационные ресурсы становятся важным компонентом в системе управления различных уровней. Постоянно растет зависимость общества и ее элементов от эффективности использования и применения информационных ресурсов. Они входят в общество наравне с традиционными углеродными, энергетическими и другими ресурсами. Информационные ресурсы устанавливаются как самообразующая система и требуют устойчивое и стабильное существование общества. В целом, информационные ресурсы – это сложный динамичный развивающийся «организм», требующий устойчивого функционирования, а также защиты от воздействия внешней среды и внутренних противоречий. Такая задача очень сложная и не может решаться путем простого упрощения показателей надежности, отказоустойчивости или безопасности. Необходим новый подход с внедрением биометрических параметров, которые повсеместно (по направлениям) имеют быть место. Внедрение биометрии для управления допуском к информационным ресурсам совсем новое перспективное направление. Обеспечение живучести всей биометрической инфраструктуры в целом – сложная проблема, решение которой требует материальных и интеллектуальных затрат. Повышение живучести функционирования биометрической системы в целом позволит произвести сдерживание и блокирование средств, методов, способов неблагоприятного и несанкционированного воздействия свести к минимуму уничтожение, копирование, тиражирование, внесение ложной информации в информационные ресурсы и их потоки, циркулирующие в различных видовых системах.

Проблемы применения биометрических технологий, их безопасность решаются на следующих уровнях.

Рисунок 1 – Уровневое распределение биометрических технологий

Обеспечение функционирования предлагаемых уровней заключается в следующем:

1. Анализ построения биометрической системы.
2. Выявление уязвимости биометрических параметров.
3. Анализ системных угроз:
   несанкционированное применение биометрии;
   некорректное использование компьютерно-аппаратных устройств;
   ошибки пользователей и администраторов;
   несанкционированное применение или подделка параметрических характеристик биометрии и антропометрии;
   нанесение ущерба биометрии физическим способом.
4. Оценка уже существующего уровня допуска к информационным ресурсам.
5. Разработка биометрической политики, направленной на целостность информационных ресурсов.
6. Формирование требований к решению применения различной биометрии.
7. Разработка перспективных биометрических проектов.
8. Гибкий и жесткий контроль за применением биометрических параметров.

Биометрической системе, как сложной системе, присуща определенная избыточность, адаптивность, отказоустойчивость и живучесть. Биометрическая живучесть подразумевает свойство системы адаптироваться к условиям функционирования допуска к информационным ресурсам, противостоять воздействиям. Наличие функционирования живучести и ее обеспечение позволяет снизить затраты на средства биометрии и повысить защиту информации в целом.

Механизмы обеспечения функционирования живучести представлены на рисунке 2.

Рисунок 2 – Механизмы обеспечения функционирования живучести биометрической системы

Исходя из рис. 2, можно сделать вывод, что поддержание функционирования живучести биометрической системы основывается:

1. Мультифакторной применимостью биометрии, которая опирается на применение нескольких биометрических параметров в виде их суммы (рисунок 3)

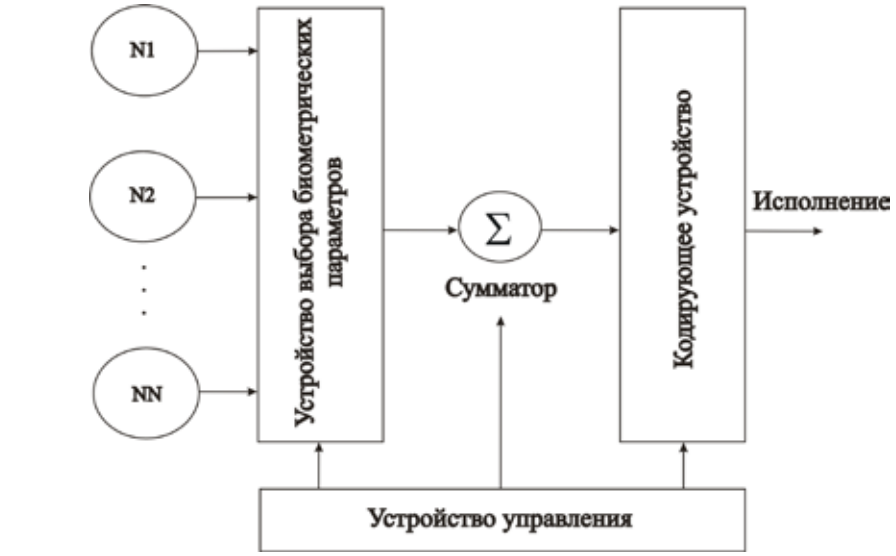

Рисунок 3 – Суммирование биометрических параметров

Таким образом, если хоть один из параметров выходит из системы, функционируют другие, что повышает живучесть.

2. Наличием единоличных биометрических параметров.

Единоличные биометрические параметры – принадлежат только одному человеку, их подделка без физического насилия невозможна, что тоже поддерживает живучесть системы по заданным требованиям. Разработка требований для функционирования биометрической системы основывается на модели, представленной на рисунке 4.

Рисунок 4 – Модель функционирования биометрической системы по требованию

Выбор требований основан на основных характеристиках y_n.

Выбор первой характеристики y_1 производится из множества M – существующих биометрических характеристик S, рисунок 5.

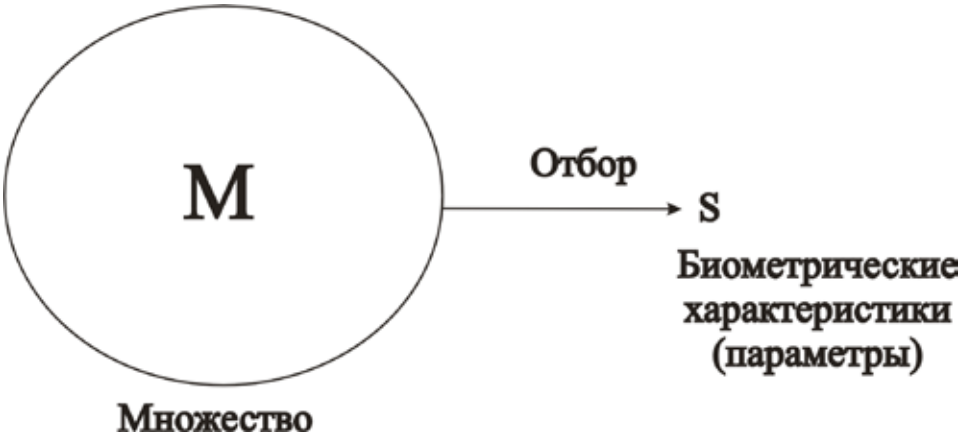

Рисунок 5 – Выбор биометрической характеристики (параметра)

S – не должен повторять (идентичность) других пользователей (личностей) ,отсюда требование:

$$S_1 \neq S_n \quad \text{(формула 1)}$$

Вторая характеристика y_2 – распознаваемость К, то есть совпадение предъявляемой $K_{пред}$ и $K_{заявл}$, заявленной в базу данных. Отсюда требование:

$$K_{пред.} = K_{заявл.} \quad \text{(формула 2)}$$

Третья характеристика y_3 – точность распознавания Q, то есть вероятность Q должна быть высокой, поэтому требование будет следующим:

$$Q \to 1 \quad \text{(формула 3)}$$

Четвертая характеристика y_4 – предлагается в виде оценки сложности (невозможности) подделки μ, то есть вероятность подделки минимальна, исходя из этого требование формулируется:

$$\mu << 1 \quad \text{(формула 4)}$$

По разработанным требованиям (табл. 1) можно производить оценку функционирования системы, конструирования, живучести.

Таблица 1

Требования для оценки функционирования системы

N	Характеристики				Требования			
	y_1	y_2	y_3	y_4	y_1	y_2	y_3	y_4
1	S	K	Q	μ	$S_1 \neq S_n$	$К_{пр}=К_з$	$Q \to 1$	$\mu < 1$
2	Произв.	Сравнение	Вероят.	Вероят.	100%	100%	70%	80%

3. Эшелонированное применение биометрических параметров.

Поскольку информационные ресурсы имеют различную степень защиты, которая зависит от категорийности сегментов, входящих в защищаемые информационные ресурсы, очевидно, что, чем больше количества применений биометрических характеристик, тем меньше вероятность несанкционированных действий (НСД). Предлагается структурно расположить биометрические рубежи аутентификации, рисунок 6.

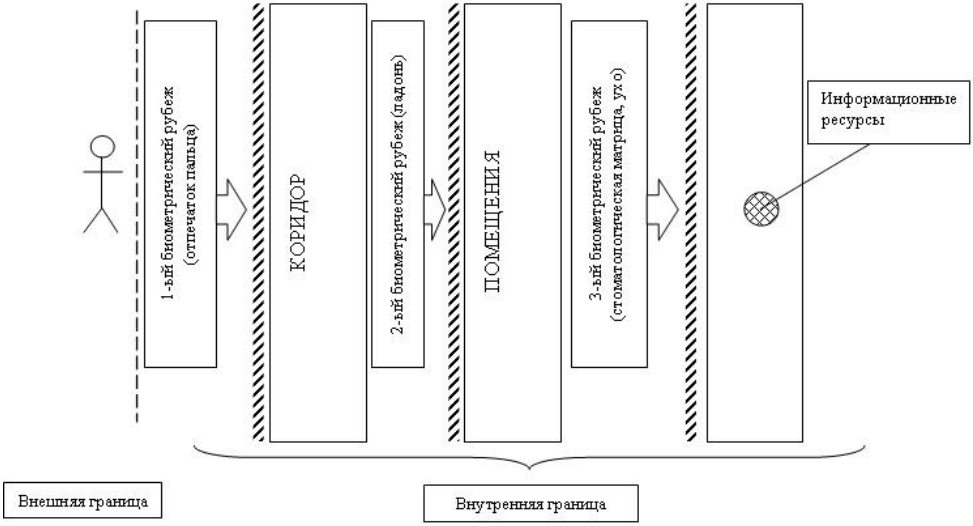

Рисунок 6 – Эшелонированное использование биометрических характеристик (параметров)

Однако для надежного функционирования биометрической системы, поддержания её в высокой живучести, необходимы дополнительно классические приёмы, такие как:

- техническая надежность устройств и элементов биометрической системы;
- гибкость системы с возможностью наращивания биометрических характеристик;
- расширенная и ранняя диагностика функционирования системы.

Все это в совокупности (рис. 2) позволяет поддерживать живучесть биометрической системы и защищать информационные ресурсы с заданными требованиями.

Литература

1. Брюхомицкий Ю.А. Вероятностный метод классификации биометрических параметров личности. // Материалы X Международной научно-практической конференции «Информационная безопасность». Часть 1 – Таганрог. Издательство ТТИ ЮФУ, 2008. – 318с.
2. Трошков А.М., Трошков М.А. Защита кодированной биометрической информации на основе свойств структуры металл-окисел-полупроводник ротовой полости человека. // Сборник научных трудов III НПК «Российская цивилизация: прошлое, настоящее и будущее». «ООО Мир данных», 2010. Ставрополь. – 410 с.
3. Трошков А.М. Аутентификация пользователя по фрагментам биометрического параметра – передней поверхности ушной раковины слухового анализатора. // Сборник научных трудов II межрегиональной НПК (часть 2). МГУПИ, изд. «Мысль», 2009. – 240 с. Москва – Ставрополь.
4. Трошков А.М., Трошков М.А. Свидетельство о государственной регистрации программы для ЭВМ № 2012617031 «Информационная система аутентификации личности по биометрическим характеристикам». Заявка № 2012614575. Зарегистрировано в Реестре программ для ЭВМ 6 августа 2012.
5. Трошков А.М., Трошков М.А., Горденко Д.В., Кондрашов А.В. Эшелонированная биометрическая защита. // Электронный журнал «Исследования в области естественных наук». – ноябрь, 2012. [Электронный ресурс]. URL: http://science.snauka.ru/2012/11/3019.
6. Додонов А.Г., Горбачин Е.С. Живучесть компьютерных систем и безопасность инфраструктуры. // Издательство ТТИ ЮФУ, 2007, №1 (76). – 238с.