К.т.н. Трошков А.М., к.э.н. Кузьменко И.П.

Ставропольский государственный аграрный университет,

Российская Федерация

КОНЦЕПЦИЯ ПОСТРОЕНИЯ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ

Существующая законодательная и нормативно-методическая база по биометрическим характеристикам человека для безопасности информационных технологий недостаточна и имеет несовершенную системность. К основным недостаткам можно отнести:

- отсутствие системности и методологии построения биометрической идентификации/аутентификации для управления доступом к защищаемым информационным ресурсам;
- недостаточной изученностью всех возможных биометрических характеристик человека;
- несовершенной моделью биометрической системы;
- статический подход к оценке управления доступом.

Раскрытые недостатки позволяют говорить о необходимости развития биометрической системы идентификации/аутентификации для ограничения доступа к информационным ресурсам различного направления.

Однако биометрическая система практически не исследована особенно на направлении систематизации биометрических параметров и их применения с целью защиты информации. Недостаточно глубоко изучена концепция управления доступом к информационным ресурсам различного направления.

Исходя из этого, предлагается систематизировать биометрическую систему защиты и управления доступом к информации. Методологический подход к построению биометрической системы и оценки ее функциональности предполагает следующие определения, представленные на рис. 1.

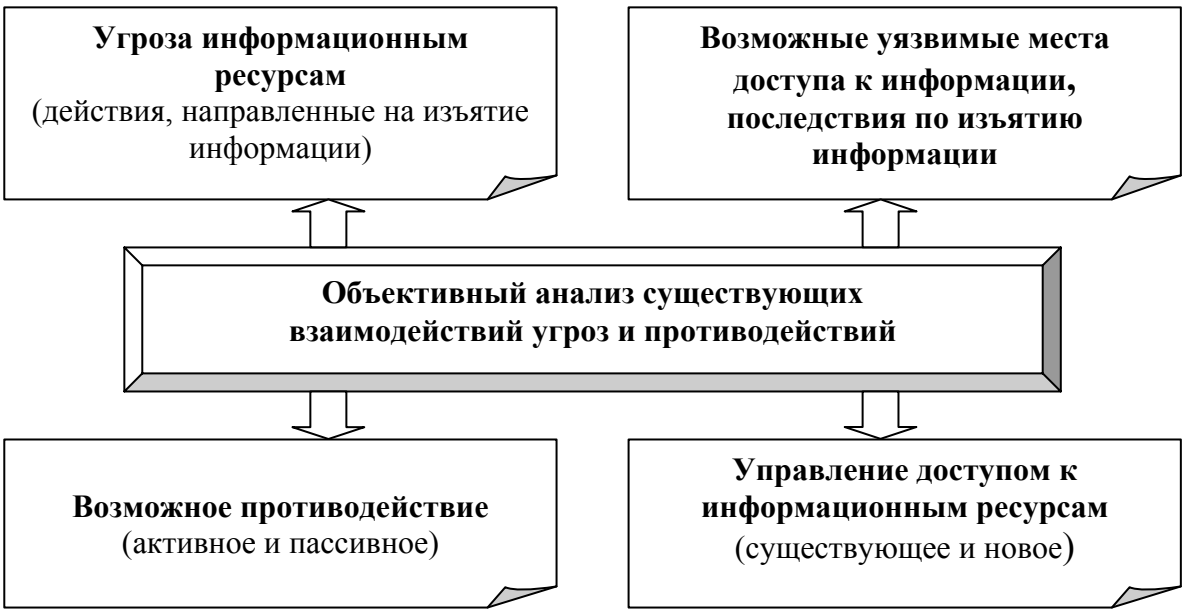

Рис. 1. Методологический подход к построению биометрической системы

Проведя анализ существенных взаимодействий угроз и противодействий, можно сделать вывод, что сравнение угроз и противодействия ведет к последствиям, представленным на рис. 2.

Рис. 2. Последствия взаимодействия

Для оценки состояния и последствия взаимодействия (рис. 2), выбираются следующие показатели:

1. Ущерб системы

$$S = \sum_{i,j,k=1}^{I,J,K} P_{ij} \cdot P_k \cdot I \,, \qquad (1)$$

где P_{ij} – вероятность противостояния системы;

P_k – вероятность уязвимости системы;

I – максимальный ущерб системе.

2. Готовность противостояния систем

$$N = \sum_{n,m,p=1}^{N,M,P} P_n \cdot P_m \cdot P_p \,, \qquad (2)$$

где P_n – вероятность реагирования системы;

P_m – вероятность появления угрозы;

P_p – вероятность готовности системы.

3. Действие угрозы

$$K = \sum_{h,q,v}^{H,Q,V} P_h \cdot P_q \cdot P_v \,, \qquad (3)$$

где P_n – вероятность подготовки к угрозе;

P_m – вероятность готовности условий к угрозе;

P_p – вероятность намерений атаковать систему.

Таким образом, если рассматривать информационные ресурсы, как мишень, то исходя из (1–3), формируется диаграмма, представленная на рис. 3.

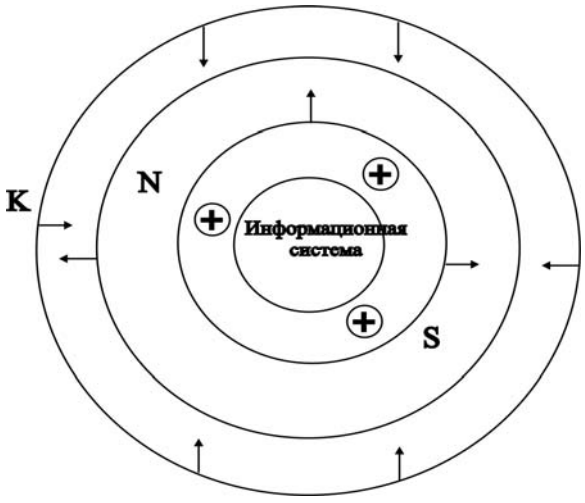

Рис. 3. Диаграмма (мишень) воздействия на ресурсы и противодействия

Из рис. 3 видно, что воздействие угроз $K(\overset{+}{\rightarrow})$ на информационную систему (ресурсы) может осуществляться со всех сторон $\alpha = 360^\circ$, противодействие и готовность $N(\overset{+}{\leftarrow})$ должны осуществляться в противоположном от k направлении с обороной 360°.

Ущерб системы S будет оцениваться, как

$$S = K(\overset{+}{\rightarrow}) \oplus N(\overset{+}{\leftarrow}). \qquad (4)$$

В идеальном случае при нейтрализации $K(\overset{+}{\rightarrow})$ и $N(\overset{+}{\leftarrow})$, результат $S = 0$. Однако в реальных ситуациях значения K и N не однозначны и могут иметь перевес сил, то есть в различные стороны. Поскольку предлагается рассмотреть для защиты информации биометрическую аутентификацию/идентификацию, то концепция управления доступом к информационным ресурсам S будет иметь биометрическую направленность, представленную на рис. 4.

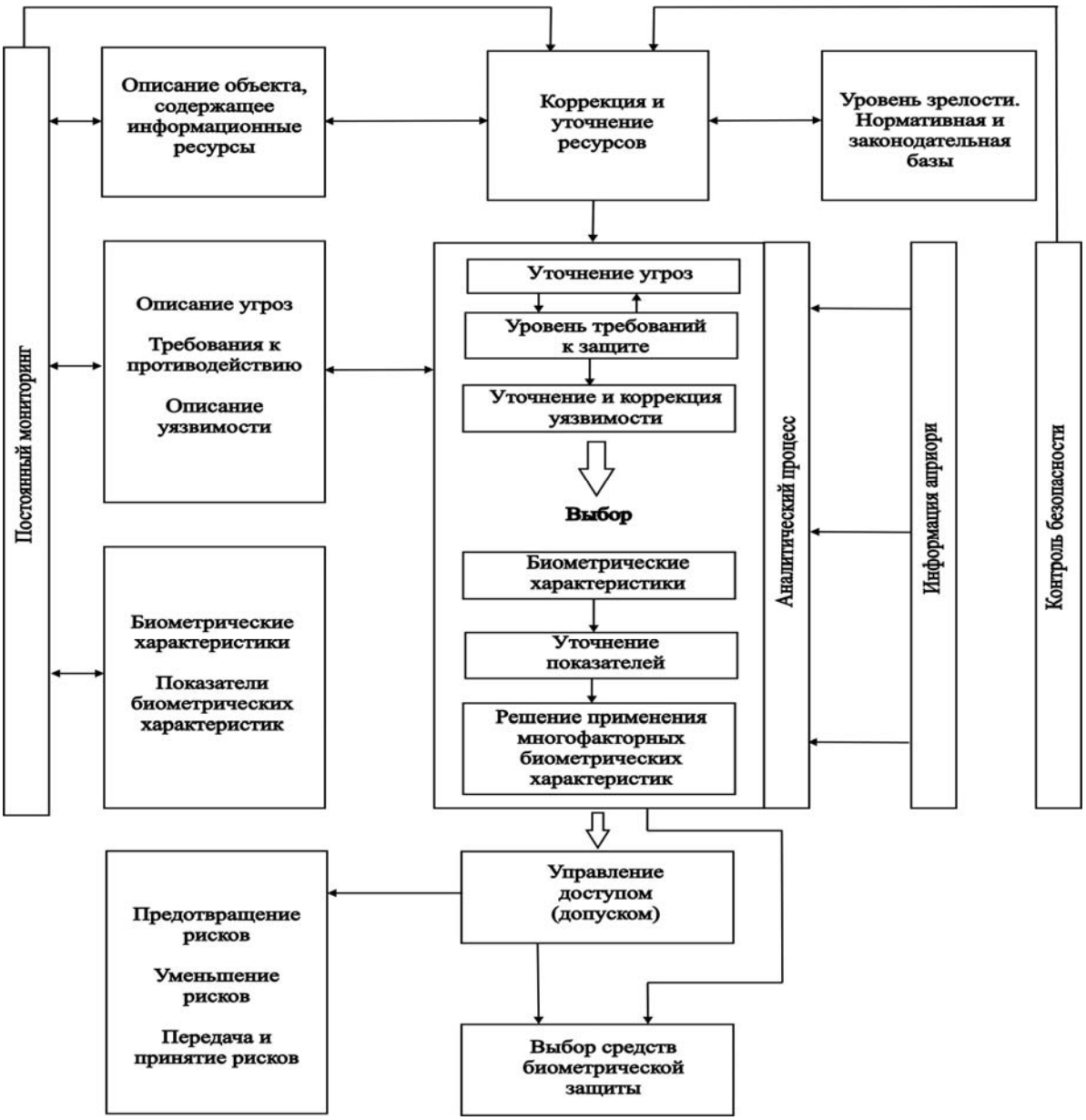

Рис. 4. Концепция управления доступом на основе системного применения биометрических характеристик

На основании предложенной концепции и методологии построения биометрической системы с целью управления доступом к информационным ресурсам разработана модель системы, представленная на рис. 5.

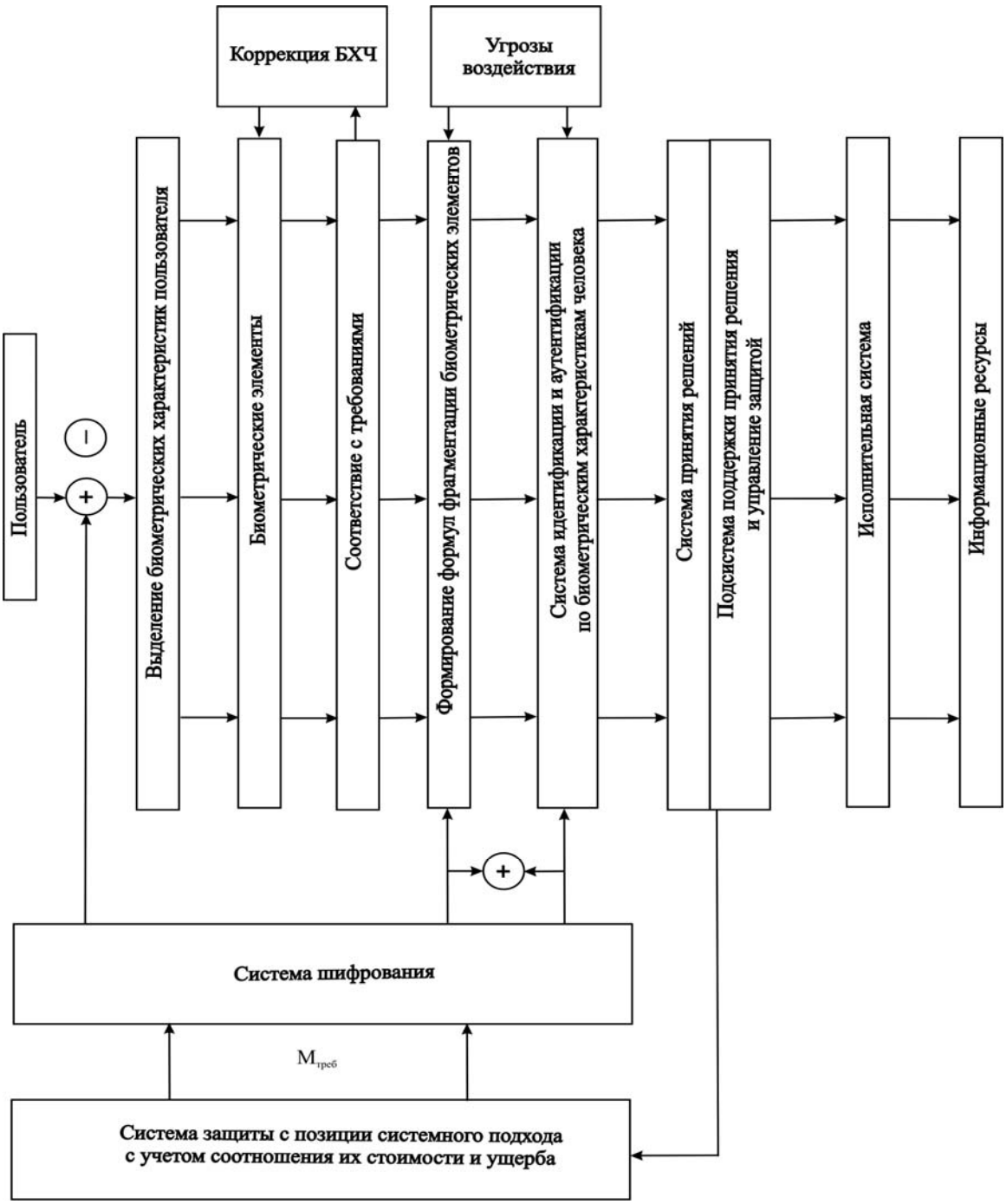

Рис. 5. Модель биометрической системы

Основной элемент модели – это пользователь, который является главным носителем биометрической информации. Поскольку система управления доступом основана на модели биометрической системы (рис. 5), в самом начале выделения биометрических характеристик применяется мультизащита $\oplus$ и Θ, где добавляются или частично убираются известные методики и средства защиты, например, паролирование. После этого производится выбор и

выделение биометрических характеристик пользователя (в том числе и предложенных новинок). Выделенные биометрические характеристики композируются в биометрические элементы, которые контролируются на соответствие требованиям, предъявляемым к биометрии. По окончанию контроля происходит формирование биометрических формул и фрагментации, по которым выполняется работа системы идентификации/аутентификации и вырабатывается сигнальная конструкция работы системы принятия решения с учетом функционирования подсистемы принятия решения совместно с управлением защитой. Отработанная система решения взаимодействует с исполнительной системой, которая является исключительной и основана на двух позициях: «да» или «нет». На основании этих позиций осуществляется допуск к информационным ресурсам. Предлагается и третья позиция «неполное ДА», то есть из всех представленных информационных ресурсов на допуск представляют только часть или сегмент.

Предложенная концепция по обоснованию рациональных методических подходов построения алгоритма управления доступом к информационным ресурсам открывают перспективы формирования эффективной модели функционирования биометрической системы.

Список использованных источников:

1. Трошков А.М. Мульти-многофакторные биометрические характеристики аутентификации личности и система их защиты / А.М. Трошков, М.А. Трошков // V-международная научно-техническая конференция г. Ставрополь: Сев.Кав.ГТУ (Кисловодск, 2–6 мая 2012 г.).
2. Трошков А.М. 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 / А.М. Трошков, М.А. Трошков.
3. Кузьменко И.П. Информационная составляющая современных методов управления устойчивым развитием предприятия / И.П. Кузьменко // Вестник Адыгейского государственного университета. Серия «Экономика». – Майкоп: АГУ, 2012. – Вып. 2(100).