Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 9, Пенза-2014, с. 70-72 (http://www.pniei.penza.ru/RV-conf/T9/C17)

ОЦЕНКА ПОТЕНЦИАЛЬНЫХ ВОЗМОЖНОСТЕЙ АЛГОРИТМОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ С ОТКРЫТЫМ И ЗАЩИЩЕННЫМ ХРАНЕНИЕМ ИНФОРМАЦИИ

Ложников П.С. (Омск), Иванов А.И. (Пенза)

Развитие информационного общества приводит к необходимости формирования доверенной корпоративной вычислительной среды, позволяющей вести корпоративный электронный документооборот. Как правило, от корпоративных электронных документов не требуется юридической значимости, однако к ним предъявляется ряд дополнительных требований. Одним из основных дополнительных требований является способность средств формирования корпоративной ЭЦП противостоять угрозе сговора сотрудников по обмену полномочиями.

Собственник информационной системы должен быть уверен в том, что право формирования личной ЭЦП не отторжимо от личности сотрудника и не может быть им передано кому либо по сговору.

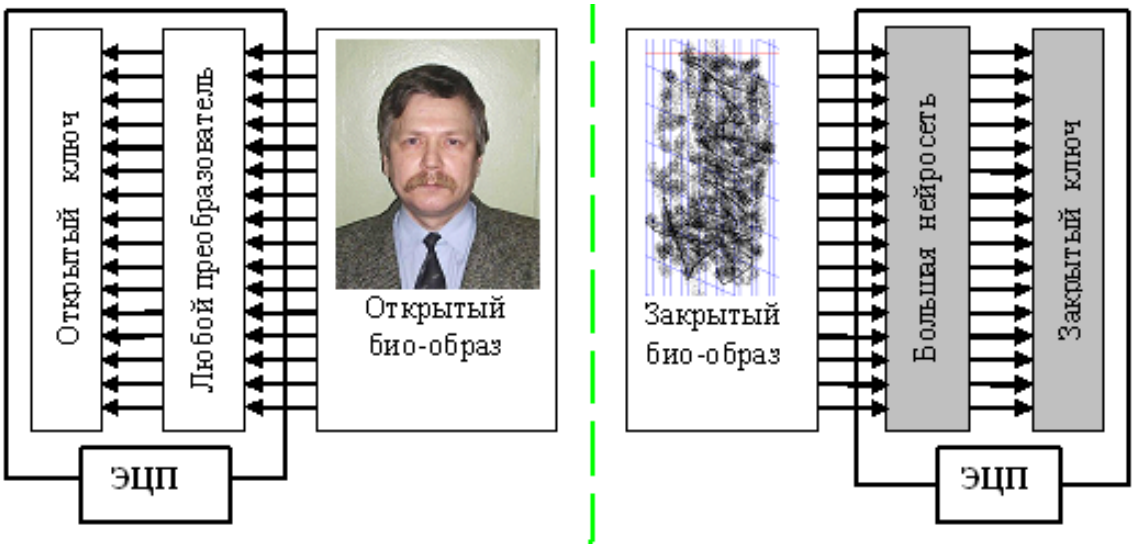

Рис. 1. Связывание открытых биометрических образов с открытым ключом (логином) и закрытого биометрического образа с закрытым ключом асимметричной криптографии формирования корпоративной ЭЦП

Очевидно, что открытый биометрический образ человека можно хранить открыто, размещая его, например, в сертификате открытого ключа (логина). При этом во время формирования корпоративной ЭЦП легальный обладатель права подписи может обратиться в корпоративный биометрический удостоверяющий центр, подтверждая свои полномочия через предъявление своего биометрического образа. Преобразователь открытой биометрии в открытый ключ может быть любым

к нему предъявляются только функциональные требования по вероятностям ошибок первого и второго рода.

Иные требования предъявляются к биометрической защите. Закрытый ключ формирования корпоративной ЭЦП должен быть надежно защищен, то есть биометрическая защита должна удовлетворять специальным требованиям [1]. В частности хищение базы нейросетевых контейнеров из корпоративной информационной системы должно быть предотвращено или должны использоваться защищенные самошифрованием нейросетевые контейнеры.

Сложившуюся ситуацию можно описать тремя вероятностями:

- P_1 – вероятность ошибок первого рода (отказ в доступе своему);
- P_2 – вероятность ошибок второго рода (ошибочный пропуск чужого);
- P_3 – вероятность реализации угрозы по извлечению знаний из защищенного контейнера с первой попытки.

Важна именно тройка вероятностей, в первом приближении их совокупность можно описать средним геометрическим:

$$\widetilde{P} = \sqrt[3]{P_1 \cdot P_2 \cdot P_3} \qquad (1).$$

Очевидно, что обеспечить низкий уровень тройки вероятностей (1) много сложнее, чем добиться низкого значения каждой из вероятности отдельно. Так же техническая задача у упрощается, если минимизировать любую пару из тройки вероятностей.

Последнее означает, что биометрические средства, обеспечивающие только целостность информации должны иметь среднее геометрическое $\sqrt{P_1 \cdot P_2}$ много меньше в сравнении с такими же средствами обеспечивающими и целостность и защиту информации.

Этот тезис подтверждается практическими оценками, вероятностных характеристик рукописных биометрических образов [2, 3]. Сети Байеса [3] не способны защищать биометрические данные, однако они обеспечивают на два порядка меньше среднее геометрическое вероятностей ошибок первого и второго рода в сравнении с искусственными нейронными сетями при обработке данных рукописных автографов.

ЛИТЕРАТУРА:

1. Язов Ю.К. и др. Нейросетевая защита персональных биометрических данных. //Ю.К.Язов (редактор и автор), соавторы В.И. Волчихин, А.И. Иванов, В.А. Фунтиков, И.Г. Назаров // М.: Радиотехника, 2012 г. 157 с.

2. Иванов А.И. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. //Монография. Пенза. Изд-во ПГУ, 2000 г., 178 с.

3. Епифанцев Б.Н., Ложников П.С., Сулавко А.Е. Алгоритм идентификации гипотез в пространстве малоинформативных признаков на основе последовательного применения формулы Байеса // Межотраслевая информационная служба. – 2013. №2 (163). – С.57-62.

Материал поступил 15.12.2014. Публикуется осуществлена по положительной рецензии д.т.н. Малыгина А.Ю.