Пензенский государственный университет
ФГУП Пензенский научно-исследовательский электротехнический институт
Пензенский филиал ФГУП НТЦ «Атлас»
Научно-производственная фирма «Кристалл»
Филиал ФГУП «ПНИЭИ» научно-исследовательское предприятие «Аргус»
Пензенское научно-исследовательское предприятие «Сталл»

Труды научно-технической конференции
Вебсайт http://beda.stup.ac.ru/RV-conf/

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ТОМ 7

Пенза 2007

УДК: 681.322

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Труды научно-технической конференции под редакцией Волчихина В.И., Зефирова С.Л.. – Пенза – 2007. Издательство Пензенского научно-исследовательского электротехнического института. Том 7. 92 с.

Рассматриваются проблемы безопасности информационных технологий. Приведенные материалы отражают дискуссию по затронутой тематике, возникшую на научно-технической Internet-конференции, непрерывно проводимой на сервере Пензенского государственного университета http://beda.stup.ac.ru/RV-conf. Представлены материалы, поступившие в оргкомитет в период с января 2006 г. по декабрь 2007 года. Том 7 содержит 21 статью, отражающие точку зрения 27 специалистов по различным аспектам информационной безопасности.

ПОЧТОВЫЙ АДРЕС ОРГКОМИТЕТА: Россия 440017, г. Пенза, ул. Красная, 40. ПензГУ. Кафедра ИБСТ, RV-конференция. E-mail оргкомитета: rv-conf@beda.stup.ac.ru, сервер конференции http://beda.stup.ac.ru/RV-conf/

СЕКЦИИ
1. Концептуальные основы информационной безопасности и проблемы информационного противоборства.
2. Информационная безопасность сложных систем.
3. Нормативное, методологическое и методическое обеспечение информационной безопасности.
4. Анализ вычислительной среды, верификация, сертификация программ.
5. Управление информационной безопасностью.
6. Системы обнаружение вторжений.
7. Аудит информационной безопасности.
8. Конфиденциальность, целостность, доступность.
9. Аутентификация: парольная, биометрическая, криптографическая.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С 3-8. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/001)

ФОРМИРОВАНИЕ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЛЕЧЕБНОГО УЧРЕЖДЕНИЯ, РАБОТАЮЩЕГО С ОЦИФРОВАННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ БОЛЬНЫХ СОЦИАЛЬНО ЗНАЧИМЫМИ ЗАБОЛЕВАНИЯМИ

Рыбалкин С.Б., Ашенбренер И.В., Иванов А.И.

Конституция Российской Федерации гарантирует всем нам доступ к информации о своем здоровье и одновременно сохранение врачебной тайны. Совместить свободный доступ к информации с сохранением врачебной тайны далеко не всегда возможно. Эти требования противоречивы, возникает классическое противоречие между свойствами доступности и конфиденциальности информации. Особую остроту эта проблема приобретает при лечения социально значимых заболеваний. В контексте борьбы с социально значимыми заболеваниями медицинскому персоналу приходится сталкиваться с нежеланием пациентов обращаться в лечебные учреждения. В частности при венерических заболеваниях больные часто занимаются самолечением или обращаются к частным «врачам», без дипломов или с сомнительной репутацией. Все это является следствием недоверия пациентов существующим механизмам обеспечения конфиденциальности медицинской информации. Последнее приводит к вероятному осложнению болезни у пациента из-за неквалифицированной медицинской помощи и к повышению вероятности инфицирования им окружающих.

Не смотря на очевидные успехи информатизации медицины, в частности ее переход на электронный документооборот, проблема обеспечения права граждан на конфиденциальность их личной медицинской информации (на врачебную тайну) только усугубляется. Электронная история болезни (любая электронная информация) гораздо более уязвима в сравнении с бумажной историей болезни. Красть бумажный архив историй болезней всей поликлиники бессмысленно – это бесполезная и крайне тяжелая работа. Электронный архив – это совсем другое дело, это уже ценная информация, размещаемая на компактном носителе. Электронный медицинский документооборот резко обостряет проблему конфиденциальности медицинской информации. Одним из путей решения этой проблемы является ее обезличивание (обеспечение анонимности пациентов). Если по электронной истории болезни невозможно определить кому она принадлежит, то шифровать информацию или тратить деньги на ее иную защиту нет необходимости. Одним из первых российских документов рассматривающих обезличивание документооборота как средство обеспечения конфиденциальности личной информации является Федеральный Закон «О персональных данных» [1].

Особенно гарантированная анонимность пациентов необходима для эффективной борьбы общества с социально значимыми заболеваниями. Только в том случае, когда больной будет абсолютно уверен в сохранении его анонимности, он будет активно сотрудничать с органами здравоохранения. В связи с этим необходимо создание специальных механизмов обеспечения анонимной идентификации заболевшего. Следует подчеркнуть, что предшествующие бумажные технологии ведения медицинского документооборота (регистрации, идентификации, выдачи справок и заключений, ведения историй болезни) не могли одновременно обеспечить полноту сведений, достоверности сведений, а так же анонимность их источника.

Кратко техническая суть проблемы отражается в противоречивом сочетании терминов «анонимная идентификация». Идентифицировать человека в обычном понимании этого термина означает узнать его, убедиться в том, что это именно тот конкретный человек с конкретным именем, фамилией, отчеством, местом жительства. Анонимная идентификация означает совсем иное. При анонимной идентификации мы должны точно знать, что перед нами находится именно тот человек, который когда то был зарегистрирован под некоторым псевдонимом (отсутствует случайная или преднамеренная подмена больного, например с целью модификации его анализов).

Заметим, что традиционными методами идентификации человека по его паспорту или по его биометрическим данным надежно обеспечить анонимность больного невозможно. Выход из создавшегося положения может быть найден только при использовании новых технологий высоконадежной биометрико-нейросетевой идентификации человека [2, 3]. Новые технологии сводятся к тому, что используется большая сеть искусственных нейронов. Большая нейросеть автоматически обучается преобразовывать биометрический образ человека (например, рисунок отпечатка его пальца как это показано на рисунке 1) в некоторый код. Например, это может быть код учетной записи потенциального больного, обратившегося в больницу изъявившего желание сдать анализы. В этой ситуации учетная запись такого потенциально больного или код его регистрации может быть следующим: «Сергей, обращение 20.04.07 в 14^{35}, г. Пенза, Куйбышева 33, врач С.Б.Рыбалкин» (смотри рис. 1). При использовании искусственной нейронной сети с 512 выходами учетная запись может иметь длину до 64 знаков.

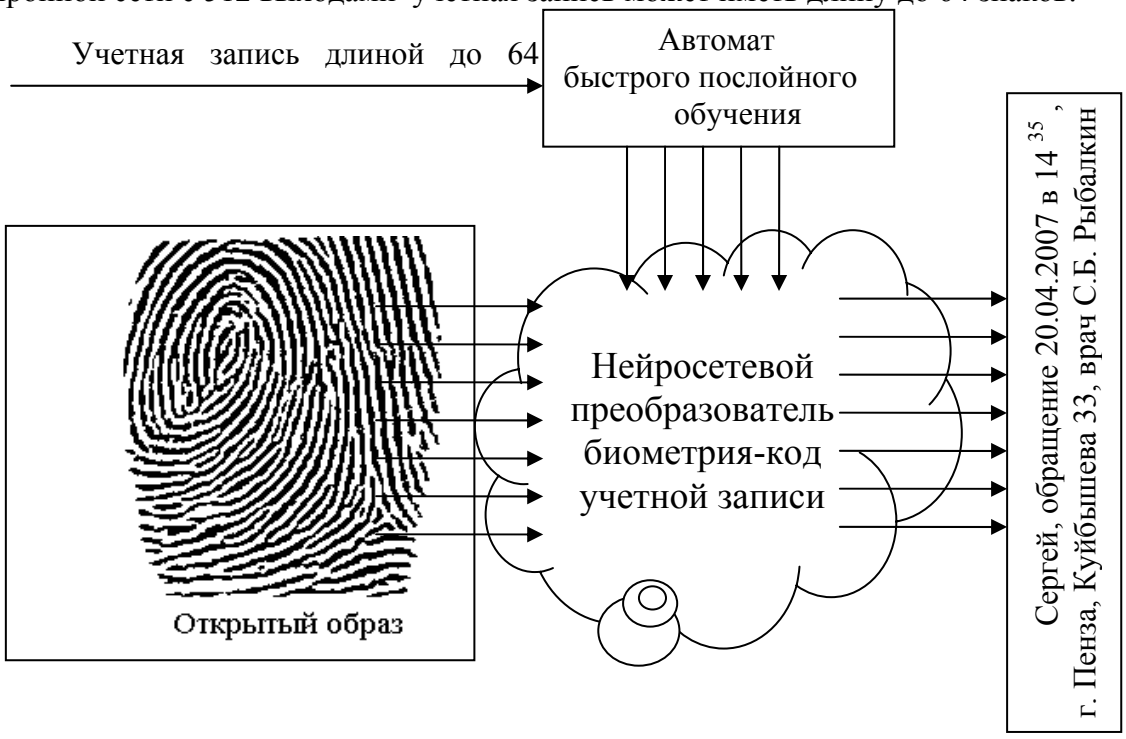


Рис. 1. Анонимная биометрическая идентификация больного с сокрытием его биометрического образа в параметрах нейросетевого преобразователя

После обучения нейронной сети биометрический образ потенциального больного гарантированно уничтожается, а большая нейросеть, обученная его распознавать и соответствующая учетная запись размещаются в электронном документе [4] в электронной истории болезни потенциального больного. Все эти предосторожности позволяют с одной стороны сохранить анонимность больного, а с другой стороны защищают врача от злоупотреблений со стороны

потенциальных больных. Потенциальный больной может попытаться выдать себя за другого человека или подменить себя другим человеком при сдаче очередных анализов. Все эти злоупотребления исключены при использовании средств высоконадежной биометрико-нейросетевой идентификации [3, 4].

Безопасная структура ведения электронного долопроизводства внутри лечебного учреждения отображена на рисунке 2. После анонимной биометрической регистрации потенциальный больной перед каждым анализом должен биометрически подтвердить себя. В нашем случае он должен предъявить свой палец для опознания в присутствии проверяющего (должностного лица принимающего от больного биоматериалы на анализ). Если пришедший сдавать биоматериалы (кровь, мочу, соскоб ткани,…) действительно тот, кто ранее зарегистрировался, то на выходах нейросети появится код, соответствующий учетной записи в направлении врача. Несовпадение кода в нескольких символах свидетельствует о незначительных ошибках нейросети из-за незначительных смещений пальца, необходимо повторно приложить палец к сканеру. Если код не читается и состоит из случайных символов, то перед нами попутка обмана или грубая ошибка (к сканеру приложен не тот палец).

Заметим, что идентификация больного может быть осуществлена при его регистрации с использованием любого биометрического образа. Так в работе [5] использование для анонимной идентификации рукописной подписи больного. Может быть использована любая из современных биометрических технологий [2], хранение биометрического образа в нейросетевом контейнере гарантирует анонимность проверяемого.

После того как биометериалы для анализа приняты и помечены учетной записью они должны поступить на обработку и через наперед заданное технологическое время будет получен результат анализа. В случае отрицательного результата (социально значимое заболевание не обнаружено) несостоявшийся больной имеет право раскрыть свою анонимность по своему паспорту и получить на свое подлинное имя заверенную справку о его состоянии здоровья на текущий момент.

В случае, если результат анализов положителен (СПИД, венерическое заболевание,…) больной встает перед дилеммой: начать лечение в медучреждении или идти к частнопрактикующему врачу. В первом случае законодательство требует от больного раскрытия его анонимности лечащему врачу при сохранении в тайне его имени для всего другого персонала лечебного учреждения. Возможны два пути реализации этого (смотри рисунок 3.)

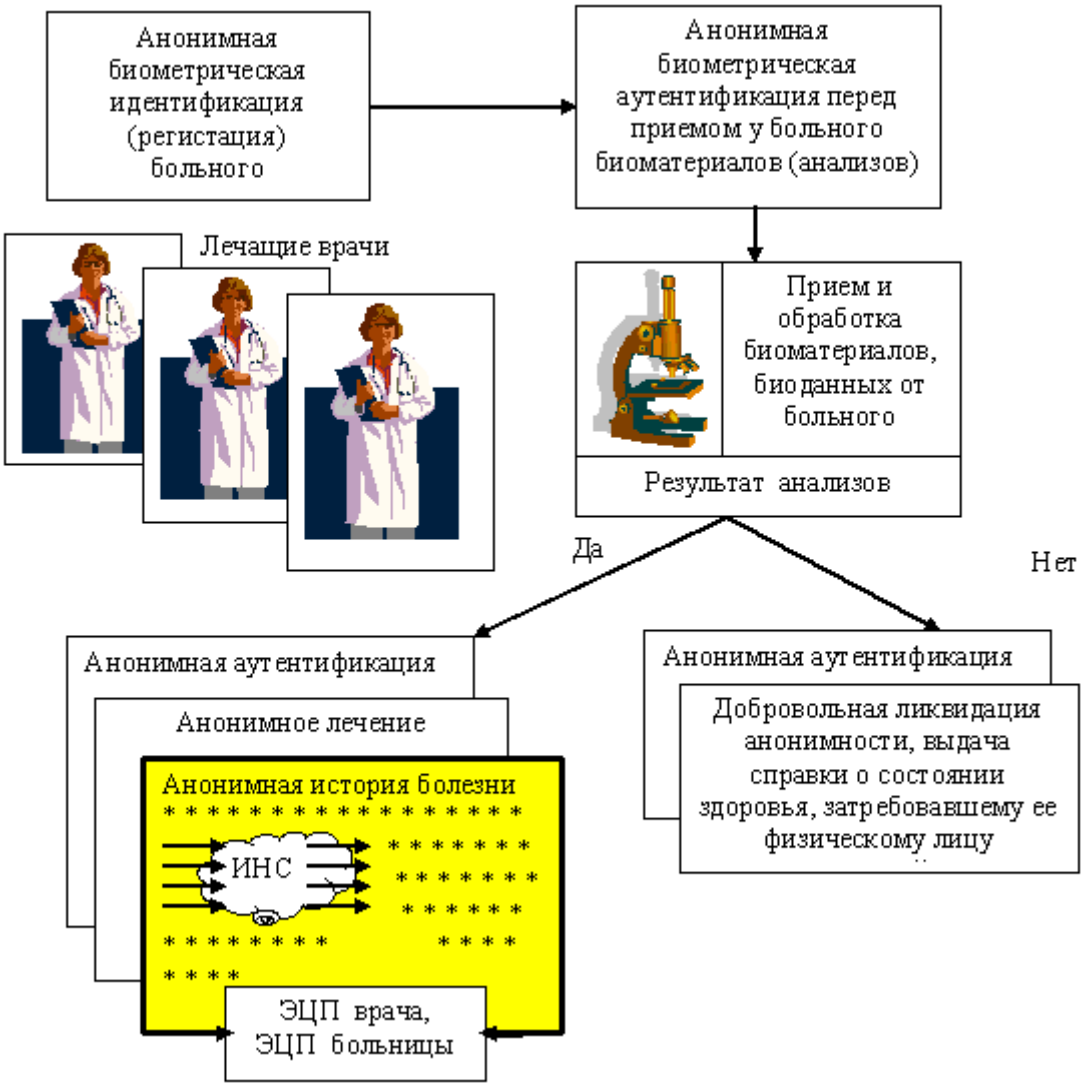


Рис. 2 . Технология обеспечения анонимности больного при ведении медицинского документооборота при высокой степени авторизации больного

Если больной не доверяет лечащему врачу, то он может обратиться к независимому нотариусу. В этом случае хранить тайну имени больного должен нотариус, однако для соблюдения буквы закона нотариус должен снять ксерокопию паспорта больного, запечатать ее в конверт, на конверте нанести требующуюся учетную запись. Все это предполагает, что у нотариуса есть не только лицензия на его деятельность, но и электронный документ из лечебного учреждения с нейросетевым контейнером тайного биометрического образа больного. Перед опечатыванием конверта нотариус должен проверить биометрию больного и нанести на конверт учетную запись выходного кода обученной нейронной сети. Больной опечатанный конверт должен передать врачу, который имеет право вскрыть его только в присутствии судьи или прокурора (оформляется, соответствующий акт вскрытия на основе, соответствующего, постановления).

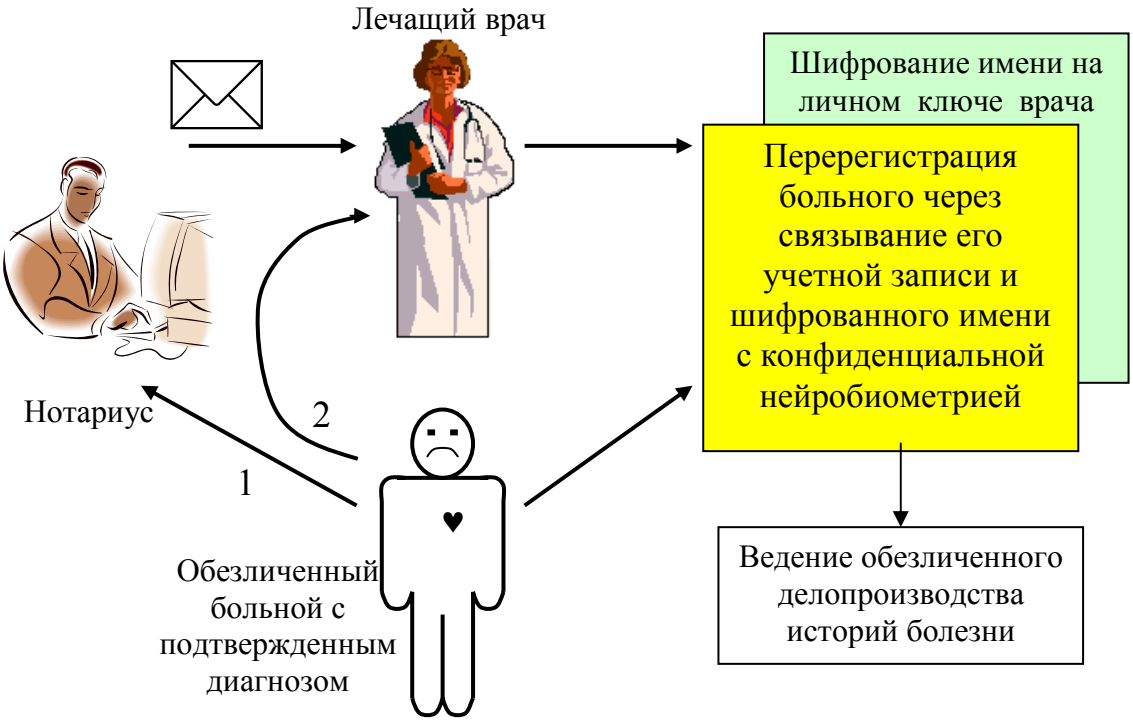


Рис. 3. Анонимная перерегистрация больного по его псевдониму и конфиденциальной биометрии с возможностью раскрытия анонимности в установленном законодательством порядке

Очевидно, что описанная выше процедура гарантированного нотариусом сохранения анонимности применима только для ВИП персон и людей неадекватно сильно заботящихся о своей анонимности. Для подавляющего большинства граждан РФ клятвы Гиппократа и порядочности лечащего врача в сочетании с системой оргтехмероприятий по сохранению анонимности больного будет вполне достаточно. В связи с этим большинство граждан будет открывать свою анонимность лечащему врачу, который должен зашифровать эту конфиденциальную информацию на своем личном ключа формирования ЭЦП, либо на производном ключе от ключа формирования ЭЦП врача. Тогда эта конфиденциальная информация будет присутствовать во множестве электронных документов медицинской отчетности, однако раскрыть ее (расшифровать шифротекст) сможет только лечащий врач. Естественно, что в этой цепочке сохранения анонимности пациентов лечащий врач начинает играть главную роль. То есть лечащий врач должен быть обеспечен средствами безопасного хранения его личного ключа, например в форме того же нейросетевого преобразователя биометрия-код, выполненного в мобильном (носимом в кармане) варианте в соответствии с требованиями нашего национального стандарта защиты информации [3].

Таким образом, требования Закона «О персональных данных» [1] технически выполнимы в контексте ведения медицинского документооборота. При этом обычное шифрование на общем ключе всех данных делает медицинский документооборот практически бесполезным. Выход только один – необходимо привлекать новые технологии высоконадежной биометрико-нейросетевой защиты информации. Традиционные технологии криптографической защиты информации при массовом использовании становятся слишком тяжелыми. Необходимо

защищать медицинскую информацию ее обезличиванием дополненным высоконадежной анонимной биометрико-нейросетевой идентификацией.

Изложенный выше подход требует формулирования в явном виде соответствующей политики информационной безопасности медицинской информационной системы для медучреждений занимающихся лечение социально-значимых заболеваний. Ниже приводим выдержки из этой политики:

1. Система должна иметь средства формирования ЭЦП врача и иного персонала;
2. Система должна быть централизованной, все рабочие станции или ПЭВМ сети должны иметь авторизованный доступ к архиву открытых обезличенных историй болезни, каждая история болезни должна являться электронным документом и подписываться последним врачом внесшим в нее запись (предыдущие ЭЦП в теле документа сохраняются);
3. Авторизация больного осуществляется только высоконадежной биометрией, биометрические данные пакуются в нейросетевой контейнер, нейросетевой контейнер хранится в заголовке истории болезни в месте с псевдонимом и начальными данными регистрации (у персонала нет средств раскрытия анонимности больного);
4. При каждом посещении или каждой процедуре приема биопроб для анализа больной анонимно авторизуется.
5. Любая анонимная авторизация больного происходит в присутствии должностного лица (врач, медсестра,…), которое подтверждает действия больного своей ЭЦП;
6. ЭЦП врача имеет удобный биометрический доступ к управлению секретным ключом, нет необходимости хранить программное обеспечение в сейфе.

ЛИТЕРАТУРА:

1. Закон РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ
2. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.
3. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
4. RU 2 292 079 - патент РФ на изобретение: «Способ идентификации человека по его биометрическому образу», авторы: Ефимов О.В., Иванов А.И., Фунтиков В.А., патентообладатель ФГУП «ПНИЭИ» (RU), приоритет от 02.02.2005.
5. Рыбалкин С.Б., Иванов А.И. Технология биометрической идентификации, обеспечивающая анонимность больных при ведении электронных историй социально значимых заболеваний /Современные технологии безопасности 2006 г., № 3,4 (18,19), с.55-57.

Получено 15.03.2006 г. Опубликована в Интернет 20.03.2006

ОПТИМИЗАЦИЯ ВЫБОРА ЧИСЛА СТЕПЕНЕЙ СВОБОДЫ ПО КРИТЕРИЮ ХИ-КВАДРАТ ПРИ ПРОВЕРКЕ ГИПОТЕЗЫ НОРМАЛЬНОСТИ РАСПРЕДЕЛЕНИЯ ВЫХОДНЫХ ПАРАМЕТРОВ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ–КОД

Захаров О.С., Иванов А.И., Малыгин А.Ю.

Лаборатория биометрических и нейросетевых технологий Пензенского научно-исследовательского электротехнического института
Межведомственная лаборатория тестирования биометрических устройств и технологий при факультете военного обучения Пензенского государственного университета

Тестирование высоконадежных средств биометрико-нейпосетевой аутентификации выполненных в соответствии с [1] требует использования сотни тысяч и миллионы примеров биометрических образов. При этом некоторые классические проверенные на практике методики оптимизации статистических вычислений перестают корректно работать. Незначительные расхождения не оказывающие сколько-нибудь существенного влияния на выборках из 400 образов, вносят существенную ошибку при 400 000 образов.

В данной статье рассматривается проблема оптимизации числа степеней свободы при проверке гипотезы нормальности закона распределения значений статистических данных по критерию хи-квадрат.

Оптимизация числа степеней свободы обусловлена тем, что при выборе малого количества столбиков, гистограмма не чувствует изменения формы закона. Например, при использовании всего двух столбиков метод вообще не чувствует вариации распределения, т.е. половина всех данных попадает в первый диапазон, а другая половина данных попадает во второй диапазон. В случае же использования большого количества столбиков, вероятность попадания значения в интервал очень низкая. Чем больше интервалов, тем ниже вероятность попадания в интервал. Обычно при выборе числа столбиков обычно используют $m = \sqrt{n}$, где n – число экспериментов. Традиционный способ выбора числа степеней свободы (числа столбцов гистограммы) на больших выборках дает ошибку порядка 50%.

На рисунках 1 и 2 представлены аппроксимации нормального закона распределения гистограммами с выбранными нами оптимальным числом интервалов m=9 при количестве проведенных опытов n=∞ (рисунок 1) и n=100 (рисунок 2).

При этом в классических вариантах для определения закона распределения статистических характеристик число опытов принято брать порядка 300…500 [2,3]. При указанном выше числе опытов погрешности аппроксимации нормального закона (рисунок 2) (заштрихованные «треугольники») не учитываются.

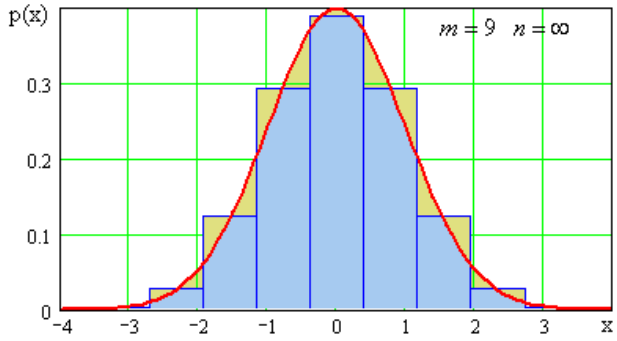


Рисунок 1 – Аппроксимация нормального закона идеальной гистограммой с оптимальным числом интервалов (степеней свободы)

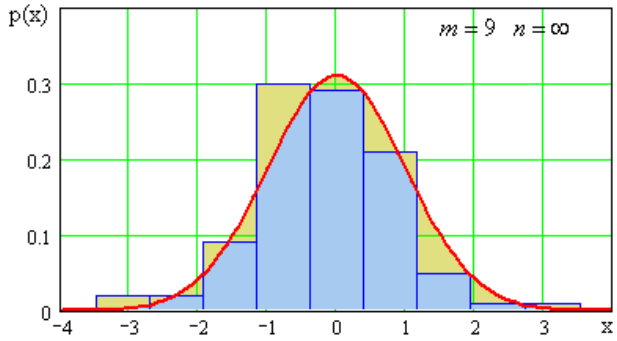


Рисунок 2 – Полученная гистограмма, аппроксимирующая нормальный закон на конечном числе опытов

В связи с тем, что нам приходится исследовать статистическое распределение выходных параметров нейросетевых преобразователей биометрия–код, имеющих значительно большую размерность (порядка 10^9 и выше), то для получения правильного решения количество опытов должно быть увеличено. В нашем случае было использовано 1500 опытов. При этом увеличивается и количество столбиков гистограммы (степеней свободы) и, соответственно, изменяется ошибка аппроксимации. Графики ошибки аппроксимации нормального закона от числа опытов приведены на рисунке 3. Приведенные на графике данные позволяют оценить и выбрать оптимальное число столбиков гистограммы (степеней свободы) для конкретного числа экспериментов. В нашем случае при n=50, m=7, E(m)=0,22. Для n=1500, m=20, E(m) =0,06.

Таким образом, из графика изображенного на рисунке 3 можно сделать вывод, что при увеличении числа опытов в 30 раз, число столбиков (степеней свободы) увеличивается почти в 3 раза, ошибка аппроксимации уменьшилась почти в 3,6 раза. Но не учитывать данную ошибку, мы не имеем права, так как число реальных опытов по определению статистического распределения выходных параметров преобразователей биометрия–код будет значительно больше 1500.

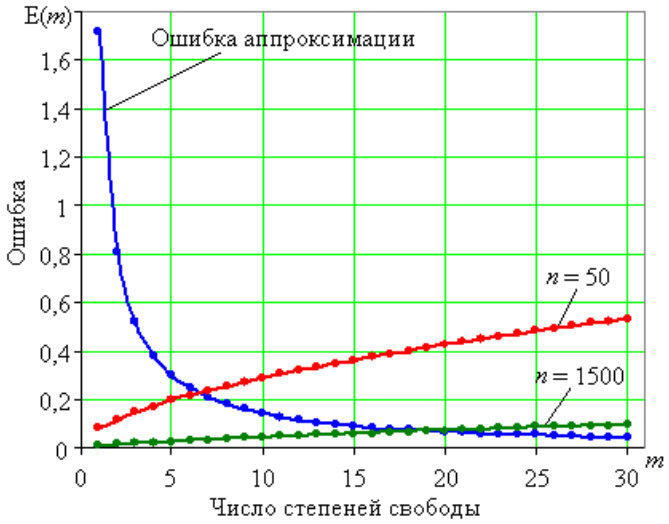


Рисунок 3 – Графики ошибки аппроксимации и ошибки из-за конечного числа опытов (n=50 и n=1500)

Для выбора оптимального числа степеней свободы по критерию хи-квадрат при проверке гипотезы нормальности распределения выходных параметров преобразователей биометрия–код нам очень важно определить связь между количеством опытов, количеством столбиков гистограммы (степеней свободы) и ошибкой аппроксимации, т.е. вычислить результирующую погрешность. Как видно из рисунка 3 погрешности носят случайный характер. Поэтому оптимальным будет взять эти оценки по модулю, а затем произвести их сложение. В результате они будут иметь явно выраженный минимум. Этот минимум и будет являться искомой точкой оптимальности (рисунок 4).

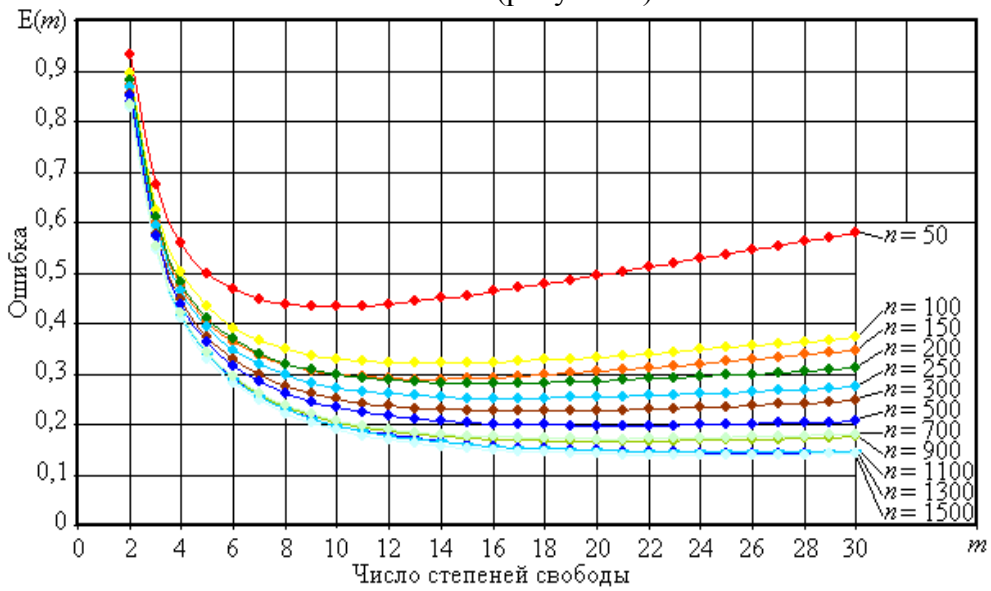


Рисунок 4– График зависимости суммарной ошибки (ошибка аппроксимации + ошибка конечного количества столбиков (степеней свободы)

В результате проведенных расчетов были получены данные, приведенные в таблице 1 и построена гистограмма (рисунок 5), позволяющие провести оптимизацию выбора числа степеней свободы по критерию хи-квадрат при проверке гипотезы нормальности распределения выходных параметров преобразователей биометрия–код.

Таблица 1 - Связь количества опытов (n) с оптимальным количеством степеней свободы (m)”

N	50	100	150	200	250	300	500	700	900	1100	1300	1500
m	9,65	13	13,3	15,5	16,56	17,18	19,95	19,92	20,3	27,34	26,5	24,1
$\sqrt{n}$	7,07	10	12,25	14,14	15,81	17,32	22,36	26,46	30	33,17	36,06	38,73

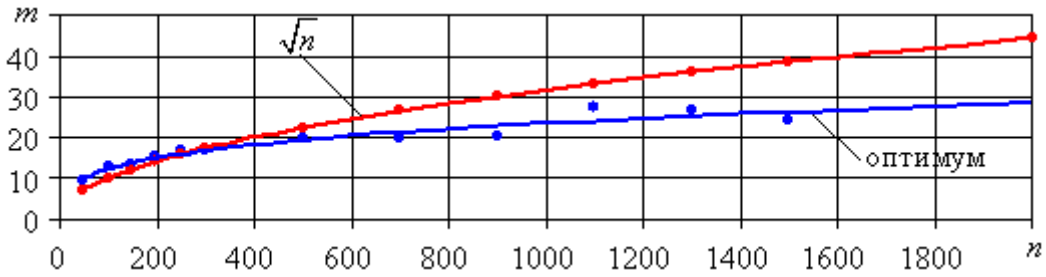


Рисунок 5 – Связь проведенных опытов с оптимальным числом интервалов (степеней свободы)

Степенная аппроксимация кривой оптимальных значений числа степеней свободы имеет следующую форму в интервале от 300 до 2000 опытов :

$$m = 3{,}454 * n^{0{,}277} \qquad (1).$$

ВЫВОД:

При проверке гипотезы нормального распределения значений для преобразователей биометрия-код выбор числа степеней свободы по правилу $\sqrt{n}$ даёт верные результаты при n порядка 300 опытов. В случае большого числа опытов выгоднее использовать выбор числа степеней свободы сделанный в соответствии с (1). Ошибка в выборе число степеней свободы для 2000 опытов составляет 33% . По $\sqrt{n}$ - 45 столбиков, а по (1) - 30. Столбиков требуется меньше, следовательно в каждый столбик попадёт больше опытов, поэтому и общая ошибка вычислений уменьшается. Благодаря данному подходу удается получать более достоверные результаты.

Литература:

1. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к высоконадежным средствам биометрической аутентификации».
2. ГОСТ Р 50779.21-2004 «Статистические методы. Правила определения и методы расчета статистических характеристик по выборочным данным. Часть 1. Нормальное распределение»
3. Точность производства в машиностроении. М.: Машиностроение, 1973. – 567с.

Получено 11.04.2006 г. Опубликована в Интернет 30.03.2006

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С 13-16... Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/003)

ИСПОЛЬЗОВАНИЕ УСЕЧЕННОГО НОРМАЛЬНОГО ЗАКОНА РАСПРЕДЕЛЕНИЯ ПРИ ОПИСАНИИ СРЕДСТВ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Надеев Д.Н.

Лаборатория биометрических и нейросетевых технологий Пензенского научно-исследовательского электротехнического института

При описании средств высоконадежной биометрической аутентификации (ВБА) [1] целесообразно использовать комплексные модели, сформированные из нескольких законов распределения [2, 3]. При формировании описания средств ВБА удобно использовать нормальный закон, который должен входить с некоторой долей участия в выходное распределение кодов нейросети. Вместе с тем используемая для статистического описания в нейросетевого базиса мера Хэмминга не может иметь значения меньше нуля. Это свойство накладывает ограничение на описывающий закон распределения – он не должен выходить за пределы длины ключа (по требованиям [4,5] длина ключа - 256 бит). Чтобы выполнить это условие и сделать модель не противоречащей реальным распределениям, снятым в практике тестирования, можно использовать закон с ограничениями на значения случайной величины, например, модуль-нормальный закон. Он определяется точно так же, как нормальный, но его значения слева и/или справа ограничены соответственно шкале меры Хэмминга. Для случая ограничения слева он записывается как

$$f(x) = 2\frac{1}{\sqrt{2\pi}\delta} e^{-\frac{1}{2\delta^2}(x-\mu)^2} \quad \text{для } x>0. \qquad (1)$$

Значения в одних и тех т же точках для модуль-нормального закона равняются удвоенному значению значения вероятности для нормального закона. Основные свойства для этого закона практически полностью повторяют нормальный закон. При приближении значения меры Хэмминга к нулю этот закон стягивается в одну точку, которая характерна для ситуации, когда мы наблюдаем ввод ключа известного ключа «Свой» легальным пользователем. Во всех промежуточных случаях эти два закона разделяют вероятностное поле, для определения вида распределения необходимо использование модели их комбинации.

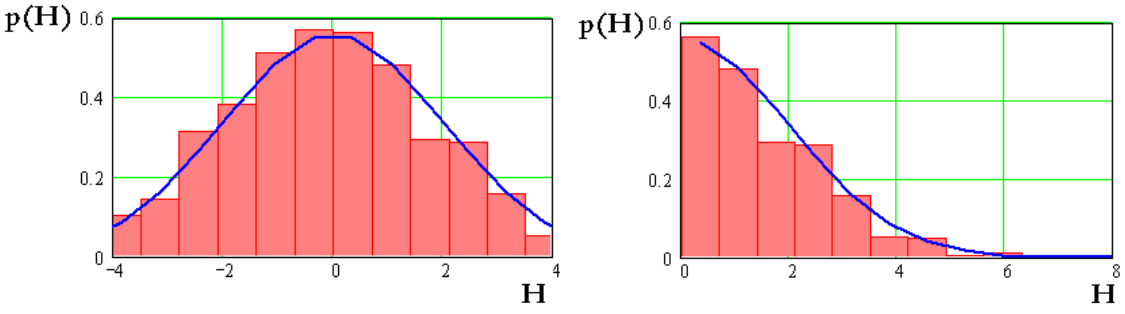


Рис. 1 – Нормальный и модуль-нормальный законы распределения меры Хэмминга выходного кода нейросетевого автомата

На рис. 1 показаны гистограммы нормального и модуль-нормального законов распределения меры Хэмминга выходного кода нейросетевого автомата. Она получается, если формирующей функцией (функцией, которая задает правило отображения значений отрицательной ветки) выступает функция модуль. Здесь хорошо видно, что происходит добавление значений по вероятности для столбцов рисунка слева и их замена одним столбцом для x>0 на рисунке справа. Это характерно для нескольких соединенных друг с другом нейронов или однослойной нейросети, обученной методом минимизации среднеквадратичной ошибки или методом максимизации качества.

Примером другой формирующей функции может быть квадратичная функция. Для значений меньше единицы квадратичная функция делает значения вероятности меньше, чем для модуля. Для выравнивания гистограммы проводится нормировка, модуль-нормальный закон с формирующей квадратичной функцией запишется как

$$f(x)=\frac{2}{\sum_{x=0}^{\infty} f(x)}\left(\frac{1}{\sqrt{2\pi}\delta}e^{-\frac{1}{2\delta^2}(x-\mu)^2}\right)^2 \quad \text{для } x>0 \qquad (2)$$

Здесь $\sum_{x=0}^{\infty} f(x)$ - сумма по всем столбцам гистограммы, нужна, чтобы избавиться от нелинейности квадратичной функции. В этом случае вероятности модуль-нормального закона равны вероятностям нормального закона с отображением по нелинейной квадратичной функции. Этот закон очень похож на полученный с помощью функции модуль, так как здесь используется только начальная часть квадратичной функции, где эти функции очень похожи.

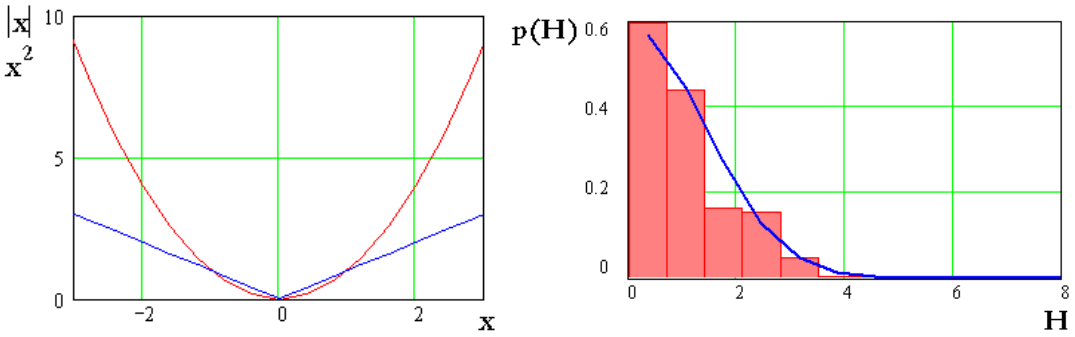


Рис. 2 – Квадратичная формирующая функция для модуль-нормального закона распределения меры Хэмминга выходного кода нейросетевого автомата

На рис. 2 показаны квадратичная формирующая функция и построенный на ее основе модуль-нормальный закон распределения меры Хэмминга выходного кода нейросетевого автомата. Столбцы гистограммы совпадают по высоте со столбцами для нормального закона, нелинейность формирующей функции вносит неравномерности в выходное распределение. Эти неравномерности характерны для радиальных сетей с гладкими дифференцируемыми нечетными функциями возбуждения, немонотонных нелинейных элементов и т.д.

Часто при статистическом приближении встает задача построения не общей модели для целой группы нейросетевых автоматов, а конкретной модели

распределения для данной нейросети. Эта задача может быть решена при использовании формирующей функции модуль, нелинейно искаженной на участках заданной длины. Получается модуль-нормальный закон, который можно записать как

$$f(x)=\frac{1+\Gamma(x)}{\sum_{x=0}^{\infty} f(x)}\frac{1}{\sqrt{2\pi}\delta}e^{-\frac{1}{2\delta^2}(x-\mu)^2} \quad \text{для } x>0 \qquad (3)$$

Здесь $\sum_{x=0}^{\infty} f(x)$ играет ту же роль, что и для модуль-нормального закона с квадратичной формирующей функцией, $\Gamma(x)$ - нелинейно искаженная функция модуль на участках, длина которых может быть равной, большей или меньшей длины единицы для шкалы меры Хэмминга. Если длина нелинейного участка формирующей функции не совпадает с единичным шагом по шкале меры Хэмминга, то происходит расширение или сужение целых размерностей. Такие нецелые размерности сродни фрактальным структурам или базисам с той принципиальной разницей, что фракталы, во-первых, в классической литературе определяются размеры меньше единицы (для нейросетевого базиса же они всегда больше единицы), во-вторых, они всегда определяются для полей конечной размерности (для нейросетей эти поля становятся бесконечно размерными).

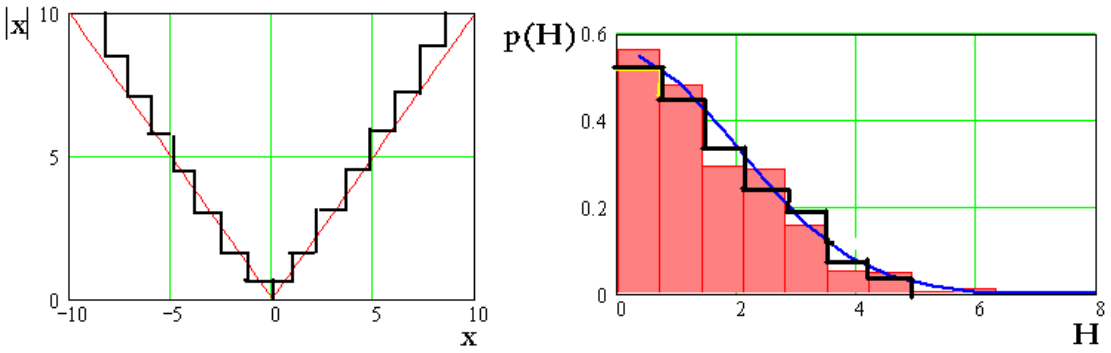


Рис. 3 – Формирующая функция неравномерного модуля для модуль-нормального закона распределения меры Хэмминга выходного кода нейросетевого автомата

Смысла в том, чтобы строить такое описание для конкретной сети, конечно, нет, его невозможно распространить на более общий случай, например, для выходных распределений данной группы нейросетей. Но получать статистическое приближение такого распределения для оценки характеристик стойкости тестируемой сети – задача, часто появляющаяся на практике, является актуальной для национальных сертификационных лабораторий и центров, работающих в соответствии с требованиями [1].

Кроме рассмотренных, можно использовать и другие формирующие (базисные) функции для преобразования нормального закона в вид, пригодный для построения модели выходного нейросетевого распределения. Независимо от того, какая из них положена в основу описывающей модели, необходимо обязательно выполнять статистическую проверку на соответствие генерируемых распределений с реальными распределениями для данного вида или класса нейросетевых механизмов защиты. Такая проверка дает гарантии устранения ошибок описывающей статистической модели на этапе ее построения. Она служит

также для обобщения модели модуль-нормального закона на данный класс или группу нейросетевых механизмов. Если такое разделение для целей описания проведено быть не может, а строить общую универсальную модель также возможным не представляется, то в этом случае можно либо изменить структуру модели, либо подобрать отвечающую требованиям базисную функцию, либо свести задачу построения общей модели к задаче поиска статистического приближения для последующей оценки характеристик стойкости тестируемого нейросетевого средства.

В итоге можно сказать, что формирующая функция модуль является наиболее предпочтительной для описания средств высоконадежной биометрической аутентификации, так как это - линейная функция, она без проблем масштабируется. Квадратичная функция чувствительна к преобразованиям и операциям над ней, после них очень сложно вернуться к начальной ее форме. Добавление неравномерностей от квадратичной функции и их появление от неравномерного модуля также могут быть использованы в построении модели выходного распределения, но они больше подходят для конкретного вида нейросети. С их помощью лучше строить статистические приближения для распределений с выходов реальных биометрико-нейросетевых автоматов, которые являются сложными многомерными статистическими моделями, не поддающимимся описанию на языке простых линейных зависимостей.

ЛИТЕРАТУРА:

1. Проект ГОСТ Р (ТК362, первая редакция) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005 г., ФГУП ПНИЭИ, ГНИИИ ПТЗИ ФСТЭК России.

2. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации: монография / В.И. Волчихин, А.И, Иванов, В.А, Фунтиков – Пенза: Изд-во Пенз. гос. ун-та, 2005. – 276 с.: ил.

3. Быстрые алгоритмы тестирования высоконадежных нейросетевых механизмов биометрико-криптографической защиты информации: монография / А.Ю. Малыгин, В.И. Волчихин, А.И, Иванов, В.А, Фунтиков – Пенза: Изд-во Пенз. гос. ун-та, 2006. – 160 с.: ил.

Получено 12.05.2006 г. Опубликована в Интернет 22.05.2006

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ ПРЕОБРАЗОВАТЕЛЯ БИОМЕТРИЯ-КЛЮЧ

Майоров А.В., Захаров О.С., Тришин А.В.

Институт Информатики и Вычислительной техники Пензенского государственного университета.
Лаборатория биометрических и нейросетевых технологий Пензенского научно-исследовательского электротехнического института

В современном мире активно развиваются мобильные технологии. Появляются новые типы устройств и изменяются хорошо известные. На сегодняшний день к мобильным устройствам можно отнести мобильные телефоны, смартфоны, КПК и планшетные компьютеры.

Мобильные устройства уже давно перестали быть роскошью и перешли в разряд предметов первой необходимости. Их используют для разговоров, заказов, деловых записей, чтения книг, просмотра видео и аудио информации, доступа к локальным и глобальным сетям. Не секрет, что пользователи часто хранят в памяти мобильного устройства конфиденциальную информацию (пароли, PIN-коды, банковские проводки, сведения об операциях с кредитными карточками, паспортные данные), необходимость защиты которой очевидна.

Один из наиболее эффективных способов защиты заключается в использовании биометрической аутентификации пользователя [1] для ограничения доступа к ресурсам мобильного устройства. В роли «естественного ключа» может выступать тайный биометрический образ (рукописное слово-пароль) человека, его голос, а при использовании специальных устройств, отпечаток пальца, сетчатка глаза.

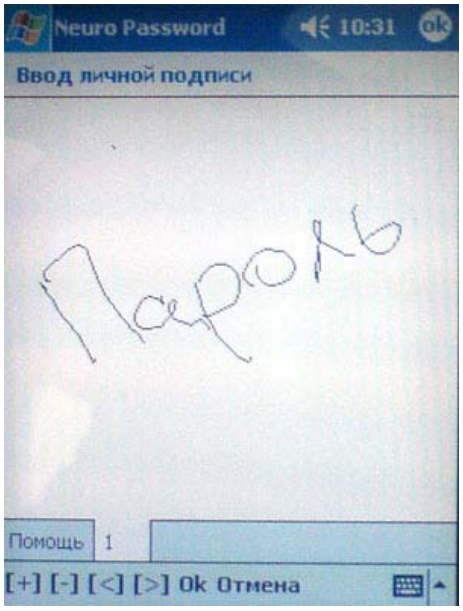


Рис 1. Вид диалога обучения ключевому слову-паролю.

Разрабатываемое средство предназначено для аутентификации пользователей мобильных устройств, работающих под управлением операционных систем Microsoft® PocketPC и Palm Inc.® Palm, а также защиты

данных от несанкционированного считывания. Стандартные средства ввода позволили организовать аутентификацию пользователя при помощи ввода рукописного пароля (рис. 1).

После активизации разрабатываемого средства в режиме ввода пароля с использованием тайного рукописного образа (рис. 2) доступ к мобильному устройству ограничивается. Первичная аутентификация пользователя производится после включения устройства, вторая и последующие – при изменении состояния устройства с пассивного (режим пониженного энергопотребления) на активное.

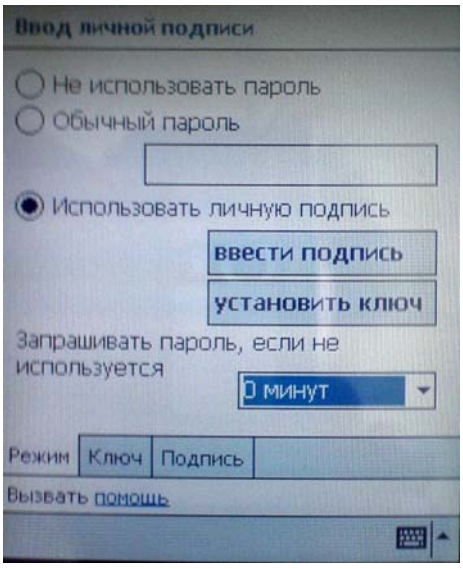


Рис2. Диалоговое окно выбора режима доступа к устройству.

Информация, хранящаяся в памяти мобильного устройства, может быть дополнительно защищена на случай физического считывания информации из памяти устройства. Файлы с данными шифруются при помощи тайного личного ключа пользователя, растворенного в параметрах искусственной нейронной сети [1]. Дешифрование возможно только после ввода правильного биометрического рукописного образа-пароля пользователя или его эквивалента в буквенно-цифровой форме.

Единственной преградой для повышения качества биометрической аутентификации при помощи рукописного ввода является низкая разрешающая способность экрана мобильного устройства. Однако последние разработки производителей мобильных устройств позволяют говорить об успешном решении этой проблемы в самом ближайшем будущем.

ЛИТЕРАТУРА:

1. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации»

Получено 2.07.2006 г. Опубликована в Интернет 20.08.2006.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С 19-.20.. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/005)

СВЯЗЬ РАЗМЕРОВ БАЗ БИОМЕТРИЧЕСКИХ ОБРАЗОВ И ИХ ЦЕННОСТИ С ТРЕБОВАНИЯМИ К ИХ ЗАЩИТЕ

Федулаев В.В., Иванов А.И., Ефимов О.В.

Лаборатория биометрических и нейросетевых технологий Пензенского научно-исследовательского электротехнического института

Защита информации является эффективной в том случае, когда материальные затраты на ее преодоление оказываются на несколько порядков выше, чем эффект от использования злоумышленником незаконно полученной им информации. Исходя из приведенного выше общего положения, рассмотрим пример формирования требований к защите баз персональных биометрических данных.

Общие предположения безопасности:

1. Ущерб от удачной атаки на биометрическую защиту 1-го пользователя – 30 000 рублей (30 000 руб. - среднее значение счета на смарт-карте с биометрической защитой в защищаемой системе);
2. Вероятность пропуска «Чужого» - для среднестатистического пользователя - $P_2 \approx 0.001$ (типичная вероятность для низкоинтеллектуальной биометрической защиты, построенной на анализе рисунка отпечатка пальца, 2D геометрии руки, рукописного почерка, голоса, 3D геометрии лица, 2D геометрии уха, анализа рисунка вен на тыльной стороне руки).
3. Злоумышленник не имеет возможности подменить биометрический шаблон на сервере системы групповой биометрической защиты (спецификация BioAPI);
4. Злоумышленник не может изготовить муляж биометрического образа (имеется защита от муляжей или ведется наблюдение за дейсвиями пользователя);
5. Злоумышленник может привлечь вычислительные ресурсы, позволяющие подбирать 10^{10} комбинаций за сутки (стоимость аренды ресурсов – 30 руб./сутки).
6. Злоумышленник может привлечь для атаки не более 10 реальных людей с реальной биометрией.

Так как, злоумышленник не может подменить биометрические шаблоны (предп. 3) и не может применить муляжи биометрии (предп. 4), он вынужден атаковать конфиденциальность базы биометрических образов с тем, что бы попытаться найти в базе людей с биометрией близкой к биометрии его 10 сообщников.

Предположим, что система имеет малые размеры и защищает базу только из 100 биометрических шаблонов. Тогда злоумышленник, получив эту базу сможет найти в ней хотя бы 1 биометрический образ, совпадающий с биометрией одного из 10 его сообщников. Соответственно, вероятный ущерб от утраты конфиденциальности базы из 100 биометрических шаблонов составит 30 000 рублей.

Для обеспечения гарантий защиты потребуем, что бы злоумышленник тратил примерно в 100 раз больше ресурсов, чем получал от удачной атаки. В этом

случае доступ к биометрической базе из 100 шаблонов должен обеспечивать не менее 10^{15} попыток подбора. То есть, необходимо использование криптографических средств защиты, подлежащих сертификацированию и имеющих длину эквивалентного ключа симметричной криптографии не менее 50 бит.

В том случае, если мы изменим пункт 2 предположений безопасности и будем считать $P_2 \approx 0.0000000000001$ (десять в минус 12 степени), то выполненные в соответствии с требованиями национального стандарта [1] нейросетевые контейнеры личной биометрии пользователей не будут нуждаться в какой-либо дополнительной защите при любых размеров баз биометрии. Даже если разместить в одну базу биометрию всех живущих на Земле людей защищать ее от злоумышленников, обладающих ограниченными ресурсами (п. 5, п.6 предположений) не требуется.

Таким образом, низкоинтеллектуальная биометрия первого поколения нуждается в сертифицированной криптографической защите баз биометрических образов. Чем больше размеры баз биометрических образов и чем выше ресурсы потенциального злоумышленника, тем длиннее должен быть ключ (пароль) доступа к защищаемой биометрической базе. Высокоинтеллектуальная биометрия, выполненная в соответствии со стандартом [1] не нуждается в дополнительной сертифицированной криптографической защите баз биометрических образов, размещенных в нейросетевые контейнеры.

ЛИТЕРАТУРА:

1. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации».

Получено 29.07.2006 г. Опубликована в Интернет 20.08.2006.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С 20-23. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/006)

АНАЛИЗ ПОВЕДЕНИЯ ЦСФС ТРЕТЬЕГО ПОРЯДКА ПРИ НАЛИЧИИ ШУМА В РЕЖИМЕ СЛЕЖЕНИЯ.

Колготин П.В., Султанов Б.В., Дорошкевич В.В., Колотков А.Ю.

Пензенский государственный университет

Объектом исследования является цифровая система фазовой синхронизации (ЦСФС) третьего порядка с равномерной дискретизацией при наличии шума в режиме слежения.

Математической моделью такой системы является следующее нелинейное разностное уравнение [3]:

$$\psi[k]-3\psi[k-1]+3\psi[k-2]-\psi[k-3]+k_1\sin\psi[k-1]+k_2\sin\psi[k-2]+k_3\sin\psi[k-3]=$$
$$=\varphi[k]-3\varphi[k-1]+3\varphi[k-2]-\varphi[k-3]-k_1 n_{ш}[k-1]-k_2 n_{ш}[k-2]-k_3 n_{ш}[k-3], \quad (1)$$

где k1=β+μ+γ, k2=-2β-μ, k3=γ, (2)

β, μ, γ - соответствующие масштабирующие коэффициенты цифрового фильтра СФС, определяющего порядок и свойства этой системы [4].

Задачей исследования является оценка зависимости коэффициента $K_{3d}=\frac{\sigma^2_{вх}}{\sigma^2_{вых}}$ ослабления дисперсии шума от коэффициентов разностного уравнения (2).

Будем рассматривать режим слежения, полагая отношение «сигнал-шум» в канале достаточно высоким (>6дБ). Это позволяет линеаризировать систему, изображенную на рис.1, так при $\psi[k]<<1$ $\sin(\psi)\approx\psi$, и поэтому звено с нелинейностью не рассматривается. При этом в силу принципа суперпозиции оказывается корректным раздельным анализ реакции системы на воздействия $\varphi[k]$ и $n_{ш}[k]$.

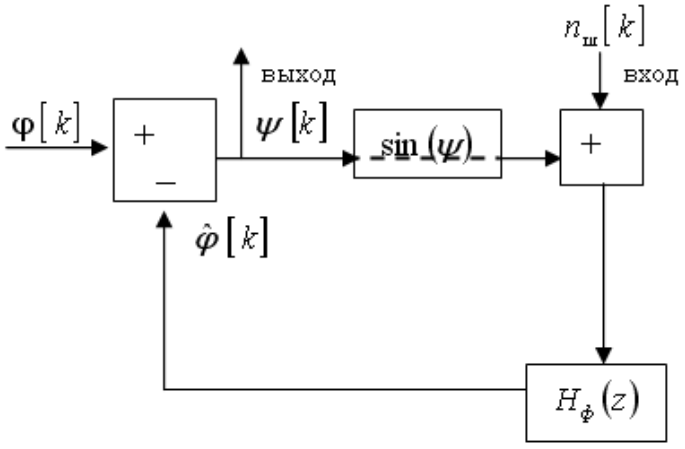


Рис. 1

Для оценки дисперсии выходного шума необходимо определить передаточную функцию линеаризированной системы $H_{3\text{ш}}(z)$, преобразующей случайную последовательность $n_{\text{ш}}[k]$ в отсчеты шума $n_{3вых}[k]$.

Для определения $H_{3\text{ш}}(z)$ в соответствии с принципом суперпозиции положим в схеме рис. 1 $\varphi[k]=0$. Тогда формируемый схемой сигнал $\hat{\varphi}[k]$ будет обусловлен реакцией системы на воздействие $n_{\text{ш}}[k]$, то есть $\hat{\varphi}[k]=n_{\hat{\varphi}}[k]$. При этом в выражении (1) слагаемые с φ[k] обращаются в ноль. На основе взаимосвязи [2] передаточной функции системы с коэффициентами описывающего ее разностного уравнения можно записать передаточную функцию системы $H_{3\text{ш}}(z)$

$$H_{3\text{ш}}(z)=\frac{k1z^2+k2z+k3}{z^3+(k1-3)z^2+(k2+3)z+k3-1} \qquad (3)$$

Во временной области алгоритм преобразования шума $n_{\text{ш}}[k]$ в $n_{3\text{вых}}[k]$ можно описать выражением

$$n_{3\,\text{вых}}[k]=\sum_{q=0}^{\infty}h_{3\,\text{ш}}[k]\,n_{\text{ш}}[k-q], \qquad (4)$$

где $h_{3\text{ш}}[k]$ – импульсная реакция линеаризованной системы, осуществляющей рассматриваемое преобразование. Последовательность $h_{3\text{ш}}[k]$ представляет собой обратное z-преобразование функции $H_{3\text{ш}}(z)$.

По определению дисперсии имеем: $\sigma^2_{3\text{вых}}=\overline{n^2_{3\text{вых}}[k]}$, или с учётом (4):

$$\sigma^2_{3\,\text{вых}}=\sum_{q1=0}^{\infty}\sum_{q2=0}^{\infty}h_{3\text{ш}}[q1]\,h_{3\text{ш}}[q2]\,\overline{n_{\text{ш}}[k-q1]\,n_{\text{ш}}[k-q2]}. \qquad (5)$$

Учитывая, что шум белый, справедливо равенство [1] :

$$\overline{n_{\text{ш}}[k-q1]\,n_{\text{ш}}[k-q2]}=\sigma^2\,x_0[q1-q2]. \qquad (6)$$

Подставляя (6) в (5), получаем:

$$\sigma^2_{3\,\text{вых}}=\sigma^2\sum_{q=0}^{\infty}h^2_{3\text{ш}}[q]. \qquad (7)$$

Сумма в (7) может быть вычислена на основе равенства Парсеваля, в соответствии с которым

$$\sum_{q=0}^{\infty}h^2_{3\text{ш}}[q]=\frac{1}{2\pi j}\oint_C H_{3\text{ш}}(z)\,H_{3\text{ш}}(z^{-1})\,z^{-1}\,dz, \qquad (8)$$

причём контур интегрирования C находится в пересечении областей сходимости $H_{3\text{ш}}(z)$ и $H_{3\text{ш}}(z^{-1})$. Подставляя в (8) выражение (3) после необходимых преобразований получаем следующее подынтегральное выражение

$$I_3(z)=\frac{(k1z^2+k2z+k3)(k1+k2z+k3z^2)}{(z-P_1)(z-P_2)(z-P_3)(1-P_1z)(1-P_2z)(1-P_3z)},$$

где P_1, P_2, P_3 – корни уравнения:

$$z^3+(k1-3)z^2+(k2+3)z+k3-1=0$$

Функция $I_3(z)$ имеет семь полюсов: $z^{(1)}=P_1$; $z^{(2)}=P_2$; $z^{(3)}=P_2$; $z^{(4)}=1/P_2$; $z^{(5)}=1/P_1$ и $z^{(6)}=1/P_2$. Проводя рассуждения, аналогичные приведённым в [1] при обосновании равенства (3.65), можно показать, что в

контур интегрирования C попадают лишь три из них: $z^{(1)}$, $z^{(2)}$, $z^{(3)}$. Вычеты функции $I_3(z)$ в этих полюсах определяются соотношениями:

$$\text{res } I_3(z)_{/z=P_1} = -\frac{(k3 + k2P_1 + k1P_1^2)(k1 + k2P_1 + k3P_1^2)}{(-1 + P_1^2)(P_1 - P_2)(-1 + P_1P_2)(P_1 - P_3)(-1 + P_1P_3)}; \quad (9)$$

$$\text{res } I_3(z)_{/z=P_2} = \frac{(k3 + k2P_2 + k1P_2^2)(k1 + k2P_2 + k3P_2^2)}{(-1 + P_2^2)(P_1 - P_2)(-1 + P_1P_2)(P_2 - P_3)(-1 + P_2P_3)}; \quad (10)$$

$$\text{res } I_3(z)_{/z=P_3} = \frac{(k3 + k2P_3 + k1P_3^2)(k1 + k2P_3 + k3P_3^2)}{(-1 + P_3^2)(P_1 - P_3)(-1 + P_2P_3)(-P_2 + P_3)(-1 + P_1P_3)} \quad (11)$$

В соответствии с теоремой о вычетах [2] правая часть выражения (8) равна сумме вычисленных вычетов (9 – 11):

$$\sum_{q=0}^{\infty} h_{3\,ш}[q] = \sum_{i=1}^{3} \frac{(k3 + k2p_i + k1p_i^2)(k1 + k2p_i + k3p_i^2)}{(1 - p_i^2)\prod_{j=1;j\neq i}^{3}(p_i + p_j)(1 - p_ip_j)}$$

Подставляя результат в (7), приходим к окончательному выражению для дисперсии $\sigma^2_{3\text{вых}}$ выходного шума ЦСФС третьего порядка:

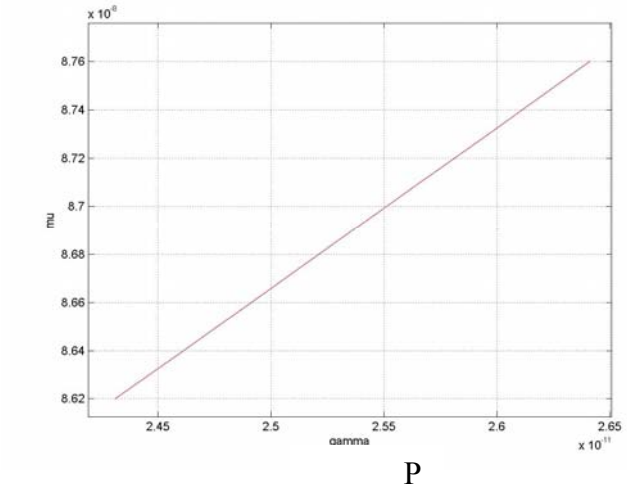
$$\sigma^2_{3\text{вых}} = \sigma^2 K_{3d}, \quad (12)$$

где

$$K_{3d} = \sum_{i=1}^{3} \frac{(k3 + k2p_i + k1p_i^2)(k1 + k2p_i + k3p_i^2)}{(1 - p_i^2)\prod_{j=1;j\neq i}^{3}(p_i + p_j)(1 - p_ip_j)}. \quad (13)$$

Результаты расчётов по формуле (13) показывают, что в области асимптотической устойчивости исследуемой ЦСФС, задаваемой системой неравенств [3]

$$0 < k_3 < 2, \quad k_1(k_3 - 1) - k_3(1 + k_3) > k_2 > \begin{cases} -k_1 - k_3 & при \quad k_3 < k_1 < 4 - k_3 \\ k_1 + k_3 - 8_3 & при \quad 4 - k_3 < k_1 < 4 + k_3. \end{cases}, \quad (14)$$



Р

величина K_{3d} уменьшается с уменьшением абсолютных значений $k1$, $k2$ и $k3$. Анализ показал, что K_{3d} актуально уменьшать до величины порядка 10^{-4}. При этом $k1$, $k2$ и $k3$ для большей точности выбираем через коэффициенты β, μ, γ, которые связаны по формулам (2). Примеры полученных зависимостей K_{3d} от масштабирующих коэффициентов в виде графиков проиллюстрированы на рисунках 2,3,4. Кривая на рисунке 2 позволяет визуально выбрать коэффициенты μ и γ (на рисунке обозначены как mu и gamma) при β=0,00045 такие, что $K_{3d} \approx 5 \cdot 10^{-4} \pm 2 \cdot 10^{-5}$. Кривая на рисунке 3 позволяет выбрать коэффициенты μ и γ при β=0,0085 такие, что $K_{3d} \approx 5 \cdot 10^{-3} \pm 2 \cdot 10^{-4}$. Кривая на рисунке 4 позволяет выбрать коэффициенты μ и γ при β=0,09 такие, что $K_{3d} \approx 5 \cdot 10^{-2} \pm 2 \cdot 10^{-3}$. Значения коэффициентов, взятые в любых точках кривых, лежат в области асимптотической устойчивости, задаваемой системой неравенств (14). Величина K_{3d} в значительной степени

зависит от выбора β и в меньшей – от двух других коэффициентов. Полученные данные позволяют обоснованно выбирать параметры системы, исходя из условий обеспечения необходимого подавления входного аддитивного шума в режиме слежения.

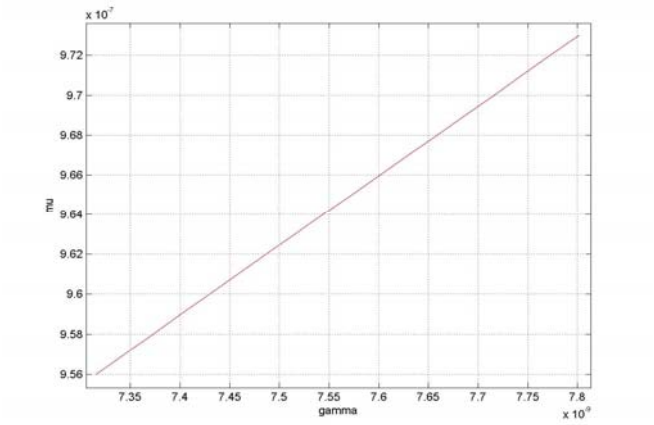


Рис. 3

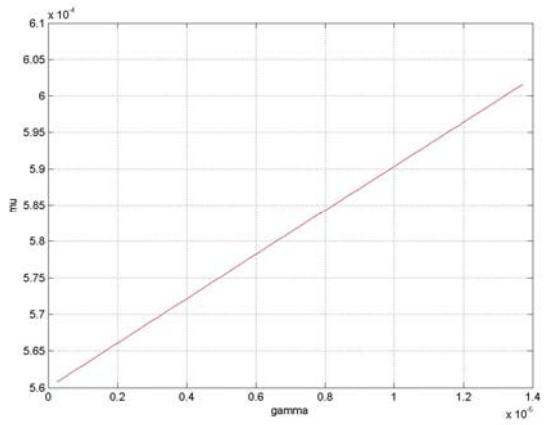


Рис. 4

ЛИТЕРАТУРА:

1. Султанов Б.В., Щербаков М.А. Анализ цифровых систем фазовой синхронизации на основе функциональных разложений Вольтера. – Пенза: Изд-во Пенз. гос. ун-та, 2002. 172 с.
2. Султанов Б.В. Основы цифровой обработки сигналов: Учеб. пособие. – Пенза: Пенз. политехн. ин-т, 1991. -84 с.
3. Дорошкевич В.В. Математическая модель системы фазовой синхронизации с равномерной дискретизацией третьего порядка // Труды научно-технической конференции. Безопасность информационных технологий – Пенза, 2005. – Том 6, Секция 5. – С. 10 – 12.
4. Султанов Б.В. Применение цифровых систем фазовой синхронизации для измерения сдвига частоты гармонического сигнала на фоне шума // Радиотехника.– 2000. - № 9. – с. 21 - 26.

Получено 20.09.2006 г. Опубликована в Интернет 27.10.2006.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С 25-27... Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/007)

УЧЕТ ЕСТЕСТВЕННЫХ КОРРЕЛЯЦИОННЫХ СВЯЗЕЙ ПРИ ТЕСТИРОВАНИИ СТОЙКОСТИ К АТАКАМ ПОДБОРА СРЕДСТВ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Малыгин А.Ю., Надеев Д.Н.

Межведомственная лаборатория тестирования биометрических устройств и технологий при факультете военного обучения Пензенского государственного университета

Важной задачей при тестировании средств высоконадежной биометрической аутентификации является построение (картины) портрета корреляционных связей, которые получаются на входе и выходе нейросетевого преобразователя биометрия/код. Такая картина не будет полной и отражать присущие этим преобразователям свойства, если мы не учтем все источники, вносящие или повышающие зависимость между выходными данными. Теоретические и практические наработки теории обучения нейростевых преобразователей и требования, установленные для средств высоконадежной биометрической аутентификации [1], дают основания предполагать, что главными источниками корреляционных связей являются:

1) структурная корреляция от соединения входов нейросети со входами соседних нейронов;
2) нейросеть может вносить свою долю зависимости между выходными кодами из-за нелинейностей и вида сети – расширяющейся или сужающейся нейросети;
3) естественных связей в почерках русскоязычных авторов задаваемые коррелятором, который повышает зависимость между выходами генератора белого шума.

Если исходить из тезиса о том, что чем больше выходов у нейронной сети, тем выше качество принимаемого ею решения, то следует стремиться делать как можно больше выходов у нейросетевых преобразователей. Наибольшее число выходов у нейросети может быть получено, если использовать нейроны с числом входов k=N/2.

Из таблицы 3 видно, что число выходов однослойной нейронной сети обрабатывающей 416 биометрических параметра может быть очень велико до $10^{123.8}$ при использовании нейронов с 208 входами. К сожалению, подавляющее большинство из $10^{123.8}$ выходов нейросети будут очень сильно коррелированны. То есть нарушается требование независимости выходов нейросети, что ставит под сомнение саму идею существенного повышения качества принимаемых решений за счет существенного увеличения числа независимых выходов.

Высокая корреляционная зависимость выходов сети обусловлена выбором большого числа входов у нейронов. Чем меньшую долю от общего числа входов занимают входы одного нейрона, тем меньше они будут перекрываться с соседним нейроном. На рисунке 1 приведены плотности распределения значений модулей коэффициентов корреляции для разного числа входов у сетей и у нейронов, соответственно, 10%, 50% и 90% от всех входов сети. Левая сеть рисунка 1 имеет 10% входов, например, 40 входов из 400. Из-за малого числа входов перекрытие их для двух нейронов маловероятно. Если верхний нейрон занимает 10% первых

входов, а второй нейрон подключается к случайным входам, то вероятность перекрытия их входов составить 0.1. В этой ситуации наиболее вероятное значение модуля коэффициента корреляции выходных данных верхнего и нижнего нейрона так же составить 0.1.

Центральная сеть рисунка 1 имеет 50% входов, например, 200 входов из 400. Из-за такого числа входов перекрытие их для двух нейронов (верхнего и нижнего) часто возникает. Если верхний нейрон занимает 50% первых входов, а второй нейрон подключается к случайным входам, то вероятность перекрытия их входов составить 0.5. В этой ситуации наиболее вероятное значение модуля коэффициента корреляции выходных данных верхнего и нижнего нейрона так же составить 0.5. Правая сеть рисунка 1 имеет 90% входов, например, 360 входов из 400. Из-за такого большого числа входов перекрытие их для двух нейронов (верхнего и нижнего) возникает очень часто. Если верхний нейрон занимает 90% первых входов, а второй нейрон подключается к случайным входам, то вероятность перекрытия их входов составить 0.9. В этой ситуации наиболее вероятное значение модуля коэффициента корреляции выходных данных верхнего и нижнего нейрона так же составить 0.9.

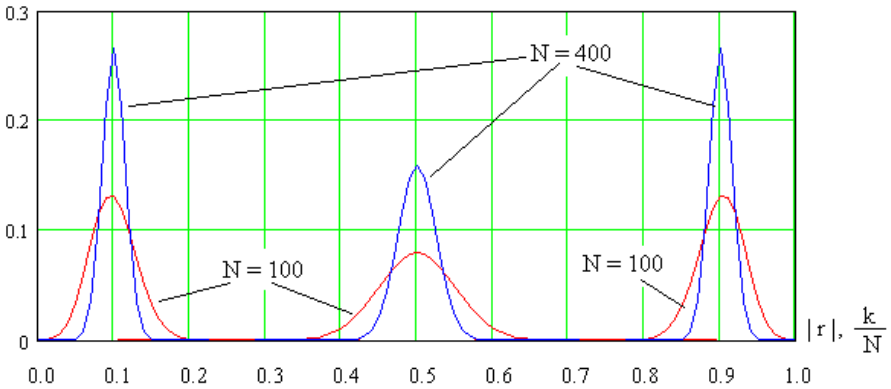


Рисунок 1 - Плотности распределения значений модулей коэффициентов корреляции для разного числа входов у сетей и у нейронов

Из рисунка 1 видно, что гипотеза независимости разрядов выходных кодов быстро разрушается по мере увеличения числа входов у нейронов. При неоправданном увеличении числа входов у нейронов возникает так называемая структурная корреляция выходных данных. Чем больше у соседних нейронов общих входных данных тем выше структурная корреляция. В пределе мы имеем так называемые полносвязные сети, которые являются наихудшим вариантом из всех возможных вариантов. Практика показывает, что желательно иметь нейроны со слабым структурным перекрытием и ограничивать среднее значение модуля коэффициентов корреляции величиной 0.15.

Свою долю корреляции вносит сама нейросеть, так как она представляет собой аналог хэш-функции, «перемешивая» входные данные и давая на выход ключи (рисунок 2). Это такое же односторонне преобразование, но только обладает особыми структурой и свойствами. Это может являться следствием настройки нелинейностей, расширяющейся или сужающейся структуры сети и т.д. Но в любом случае любая сеть обязательно дает некоторую зависимость между выходами, является с этой стороны коррелятором со своей величиной корреляции.

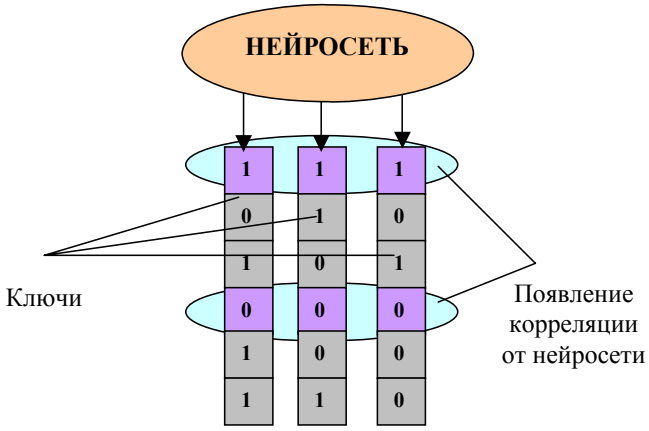


Рисунок 2 - Появление корреляции, обусловленной нелинейными элементами и видом нейросети

Измерить такой вклад в зависимость выходных кодов можно, если использовать сеть с неперекрывающимися по входам нейронами, подавая вектора со случайными данными. Такие эксперименты показывают, что рассматриваемая доля зависимости для нейросети с 416 входами и 256 нейронами не превышает 0,02-0,04. Это позволяет говорить о допустимости такой добавки в общую зависимость выходов сети, но нужно следить за правильной настройкой нелинейностей, она легко проверяется по этой же схеме.

Связи, вносимые коррелятором, мы используем для описания нейросети и векторов входных биометрических данных – для имитации биометрических данных с симметричными и асимметричными корреляционными матрицами. Для этого на вход сети устанавливается коррелятор с регулируемой величиной корреляции, мы, таким образом, задаем матрицу связанности входов. Можно выбирать различные варианты матриц связанности: знакопостоянные / случайные по модулю значения коэффициентов корреляции; случайные дисперсии и случайная знакопеременная матрица коэффициентов корреляции; ленточные матрицы коэффициентов корреляции; Марковская корреляционная матрица и т.д.

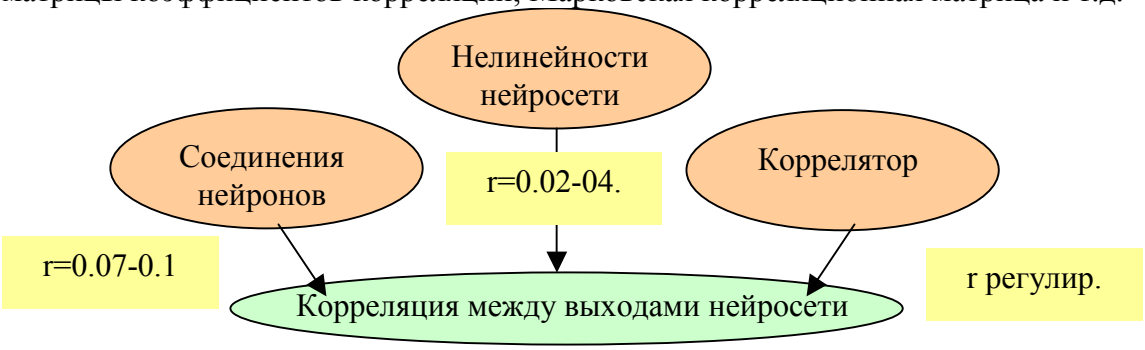


Рисунок 3 - Составляющие корреляции между выходами нейросети

На рисунке 3 показаны составляющие корреляции между выходами нейросети. Рядом со стрелками указаны величины корреляции для каждого из источников. Кроме коррелятора, где r настраивается, структура входной и выходной части сети дают суммарную величину корреляции r = 0,13-0,15 для сети 416 входов 256 выходов. Это согласуется с требованиями ГОСТ-Р для средств высоконадежной аутентификации.

ЛИТЕРАТУРА:

4. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к высоконадежным средствам биометрической аутентификации».

Получено 29.09.2006 г. Опубликована в Интернет 13.11.2006.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С 28-36. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/008)

СИСТЕМЫ ВНУТРИВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИКО-КРИПТОГРАФИЧЕСКОЙ АУТЕНТИФИКАЦИИ СЛУЖАЩИХ

А.В. Колючкин

ФГУП «Пензенский научно-исследовательский электротехнический институт»

В настоящее время в нашей стране идет бурный процесс информатизации практически всех сфер общественной деятельности, в том числе и в таких ведомствах, как: МВД, МЧС, ФНС и т.д. Хотя бумажный документооборот все еще преобладает над электронным документооборотом в силу довольно слабой распространенности последнего, объем корпоративных электронных документов удваивается каждые три года. В связи с этим все более актуальной становится задача разработки индивидуальных малогабаритных (портативных) защищенных от НСД устройств пользователя для выполнения криптографических преобразований информации в процессе информационного обмена, а также для хранения служебной информации сотрудников ведомства, в том числе в оперативной обстановке.

С развитием вычислительной техники и электронных технологий обработки и передачи информации на расстоянии, а так же согласно федеральным программам, проводимым в России, осуществился переход к электронному документообороту (ЭДО), позволившему автоматизировать многие процессы делопроизводства. В органах государственной власти России, и в перечисленных выше ведомствах в том числе, большое распространение получили системы электронного документооборота, такие как Lotus Notes и Docks Vision, обладающие большой функциональностью и удобством пользовательского интерфейса. Однако, в противоположность удобства и функциональности, обозначенные системы электронного документооборота не отвечают современным требованиям по обеспечению требуемого уровня безопасности. Следует отметить, что сделанное замечание справедливо также для других систем электронного документооборота – архитектура практически всех систем электронного документооборота, как зарубежных, так и отечественных, требует переработки с учетом современных требований безопасности. Это обусловлено следующими особенностями архитектуры программного обеспечения:

- отсутствием поддержки отечественных алгоритмов криптографического преобразования информации (для зарубежных систем электронного документооборота);
- оторванностью подсистемы обеспечения информационной безопасности от процесса создания и обработки электронного документа: электронная цифровая подпись под документом появляется в момент передачи документа по каналу связи, отсутствие меток безопасности в составе документа;
- несоответствия перечисленных систем электронного документооборота для обработки информации требуемого уровня безопасности в территориально распределенных информационных

системах ведомственного и межведомственного электронного документооборота.

Для обеспечения информационной безопасности гетерогенной территориально распределенной информационной системы ведомства должен быть использован комплексный подход, учитывающий требования живучести, адекватного уровня безопасности, возможности эволюционного развития подсистемы обеспечения информационной безопасности.

ФГУП «ПНИЭИ» имеет большой научно-технический задел в сфере решения задач по разработке систем информационной безопасности, учитывающих вышеизложенные требования. Данный задел был накоплен и успешно апробирован в ходе выполнения ряда ОКР.

Технические решения по обеспечению информационной безопасности, отвечающие современным требованиям, заключаются в создании интегрированной подсистемы информационной безопасности на базе комплексов современных технических средств, разработанных и разрабатываемых на основе высоких современных технологий и обеспечивающих, в том числе в автоматизированных режимах:

- поуровневую криптографическую совместимость;
- дистанционное управление безопасностью по рабочим каналам связи со стороны территориально-распределенного центра управления безопасностью;
- мониторинг технического состояния по рабочим каналам связи;
- проведение аудита безопасности на заданную глубину во времени;
- поуровневая иерархическая структура центров управления безопасности во главе с главным центром управления безопасностью.

В задачи центра управления безопасностью, кроме управления функционированием самой подсистемой информационной безопасности, должно входить обеспечение юридической значимости ведомственного электронного документооборота.

Эта задача решается с помощью Удостоверяющего Центра (УЦ), показанного на рисунке 1, входящего в состав центра управления безопасностью.

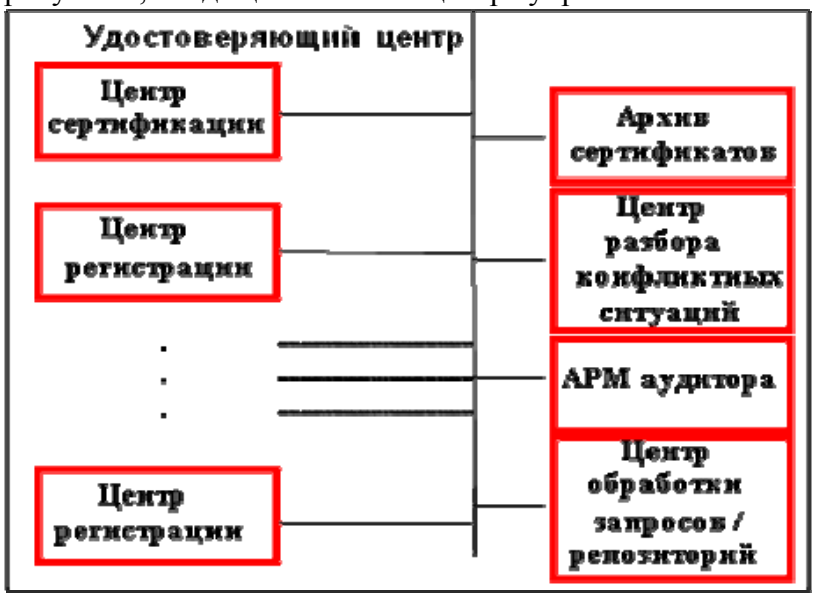


Рисунок 1 – структура удостоверяющего центра.

Основными функциями УЦ являются:

– автоматизированное управление политикой безопасности, включая управление ключами ЭЦП и сертификатами участников;
– управление индивидуальной (персональной) информацией участников;
– удостоверение подлинности ЭЦП;
– юридически значимый разбор конфликтных ситуаций.

При этом компоненты УЦ могут носить территориально-распределенный характер, а инфраструктура УЦ может иметь иерархическую, многоуровневую структуру, отражающую особенности организации связи и управления.

Исходя из определения основных функций УЦ, следует, что инфраструктура открытых ключей, управляемая со стороны УЦ, есть набор служб безопасности, позволяющий использовать и управлять техникой криптографии с открытыми ключами, включая, в том числе, собственно ключи, сертификаты участников и политику администрирования.

В настоящее время в ФГУП «ПНИЭИ» ведется разработка удостоверяющего центра по высокому уровню обеспечения безопасности от атак квалифицированных нарушителей.

В соответствии с современными требованиями по обеспечению информационной безопасности, должен использоваться дифференцированный подход к обеспечению информационной безопасности объектов информатизации: в некоторых случаях достаточным является уровень безопасности КС3, в других же случаях должен быть обеспечен уровень безопасности вплоть до КВ2 (КА).

Многоуровневая модель инфраструктуры удостоверяющих центров показана на рисунке 2.

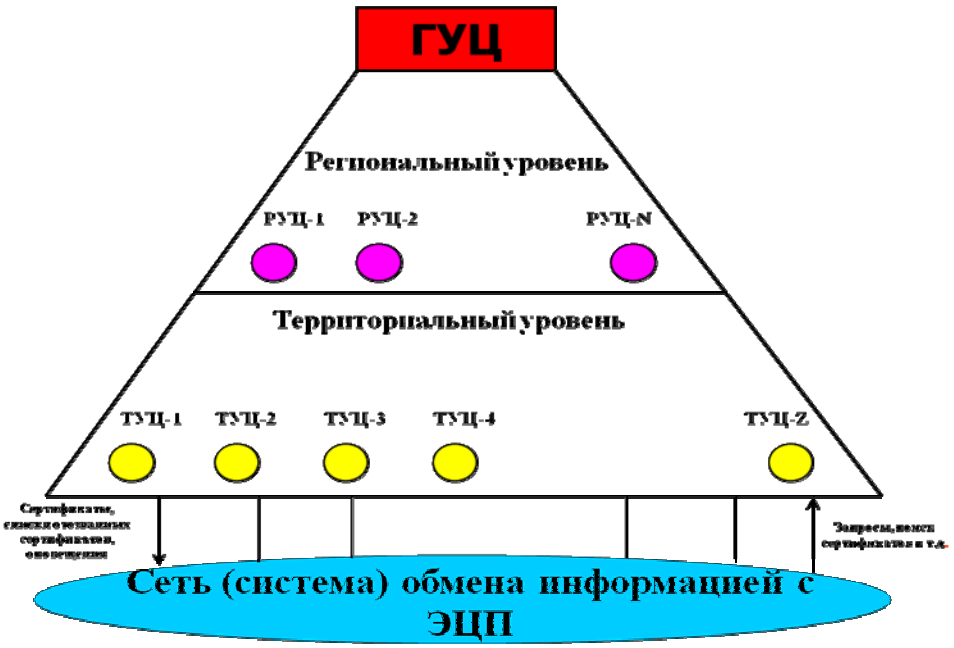


Рисунок 2 – Схема многоуровневой модели инфраструктуры удостоверяющих центров МВД России.

Однако обеспечение высокого уровня обеспечения безопасности требует, чтобы криптографические преобразования информации проходили в доверенной среде, каковой широко распространенная ПЭВМ вкупе с операционной системой семейства MS Windows не является (Windows XP сертифицирована ФСБ России только по одному из самых низких уровней – КС2). Для решения этой проблемы ФГУП «ПНИЭИ» предлагает ряд решений на базе защищенных от НСД малогабаритных вычислитель-носителях, носителях типа «Криптофлэш».

Суть изделий типа «Криптофлэш»: внешняя по отношению к ПЭВМ и операционной системе изолированная, доверенная среда.

Изделия семейства «Криптофлэш» выполнены в виде бытовых USB-Flash Drive, широко распространенных в вычислительной технике.

Внешний вид СКЗИ типа «Криптофлэш» приведен на рисунке 3.

Изделия «Криптофлэш» могут иметь в зависимости от варианта исполнения и выполняемых функций емкость встроенной Flash-памяти от 0 до 1024 Мбайт (в первом случае для выполнения процессов используется только внутренняя память микроконтроллера).

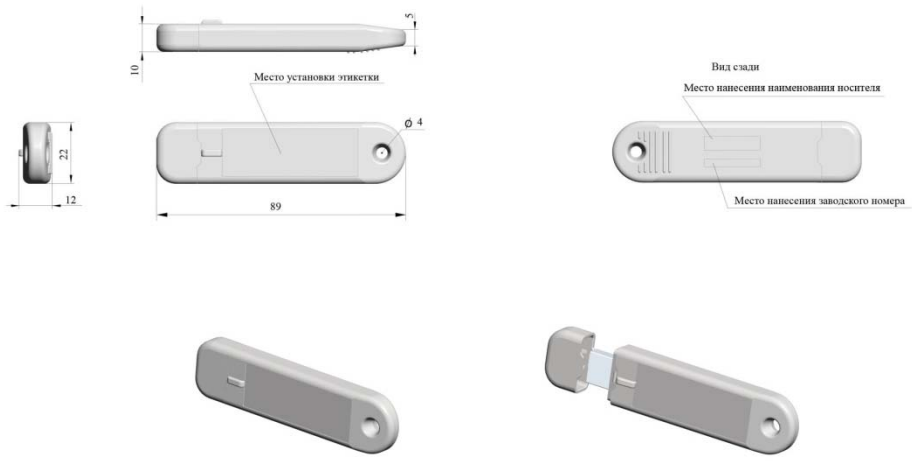


Рисунок 3 – внешний вид изделий типа «Криптофлэш»

Основные технические характеристики изделия типа «Криптофлэш» приведены в таблице 1.

Таблица 1 – основные технические характеристики изделия типа «Криптофлэш»

Архитектура	Накопитель большой емкости на базе Flash-памяти, работающей под управлением микроконтроллера отечественного производства
Исполнение	Малогабаритный корпус с USB-разъемом типа А
Емкость встроенной Flash-памяти (в зависимости от модели)	0 кбайт, 8 кбайт, 16 кбайт, 32 кбайт, 64 кбайт, 64 Мбайт, 128 кбайт, 256 Мбайт, 1024 Мбайт
Материал корпуса (в зависимости от модели)	Металл, пластмасса (монолитный и клееный корпуса)
Протокол обмена с внешними устройствами (в зависимости от модели)	USB 2.0, режим Full Speed UART USB 1.1, режим Low Speed и Full Speed
Скорость обмена с внешними устройствами USB 2.0 UART USB 1.1	 12 Мбит/с 115,2 кбит/с 1,5 Мбит/с и 12 Мбит/с
Определение типа стыка	Автоматическое
Скорость шифрования	до 256 кбайт/с при сохранении

данных	зашифрованныз данных в носителе до 100 кбайт/с при возврате зашифрованных данных в ПЭВМ
Время формирования ЭЦП	0,2 с
Время проверки ЭЦП	0,4 с
Ресурс формирования ключей (пар ключей) ЭЦП	1,2 млн. пар
Производительность хэширования информации	До 120 кбайт/сек
Габаритные размеры	86x22x12,5 мм
Вес, не более	30 г
Рабочая температура	от минус 40°С до плюс 50°С
Срок хранения данных	до 10 лет

Основными ТТХ изделий типа «Криптофлэш» являются:

- криптографическая защита информации пользователя (группы пользователей) в виде файлов или данных, а также защита несанкционированного доступа (НСД) к программно-аппаратным ресурсам изделия и к записанной информации;
- встроенные функции шифрования / расшифрования и / или вычисления и проверки электронной цифровой подписи (ЭЦП) под сообщениями (массивами) информации произвольного объема;
- функции автономного формирования ключей (пар ключей) ЭЦП во внутренней программно-аппаратной среде изделий из исходных последовательностей большого объема;
- криптографическая обработка информации согласно ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11.-94 (возможна реализация других алгоритмов по требованию Заказчика);
- энергонезависимое хранение информации с защитой от НСД с поддержкой системы организации файлов на платформах Windows 98/2000/XP, Linux, МСВС 3.0, DOS 6.22, ЗОС «Оливия».

Указанные ТТХ позволяют использовать изделия по функциональному назначению в виде:

- СКЗИ, реализующего шифрование / расшифрование информации «на проходе» по схеме: ПЭВМ→СКЗИ→ПЭВМ;
- СКЗИ, реализующего режимы предварительного шифрования при обмене информацией посредством сетей и систем общего и ведомственного пользования;
- съемного электронного диска большой емкости, защищенного от НСД;
- аналога бытовой USB-flash, защищенного от НСД;
- криптопровайдера, обеспечивающего в системах электронного документооборота (ЭДО) вычисление и проверку ЭЦП, а также хранение и формирование ключей (пар ключей) ЭЦП.

Необходимо подчеркнуть, что в рамках описанной архитектуры во всех модификациях все процессы криптографической обработки электронных сообщений и электронных документов осуществляются в изолированной и защищенной от НСД программно-аппаратной среде СКЗИ «Криптофлэш», отделенной от общесистемной и операционной среды ПЭВМ. При этом требования к последней не предъявляются и в ней могут быть применены широкораспространенные программные продукты, функционирующие, например,

в обычной операционной среде Windows, такие как система электронного документооборота типа Lotus Notes или Docs Vision. Могут быть заданы алгоритмы работы, при которых ключи, включая ключи шифрования и закрытые ключи ЭЦП, никогда не покидают и не выводятся за пределы программно-аппаратной среды носителя в течение всего жизненного цикла и могут быть неизвестны даже пользователю СКЗИ.

В вариантах исполнения по назначению криптопровайдера каждый абонент, имеющий «Криптофлэш», может на рабочем месте произвольно во времени изготавливать и менять ключи ЭЦП и может быть при этом уверен, что закрытые личные ключи вычисления ЭЦП неизвестны никому, включая удостоверяющий центр. Закрытый ключ вычисления ЭЦП может оставаться неизвестным даже самому пользователю – ключ формируется и функционирует только в изолированной среде СКЗИ, недоступной ему для непосредственного обращения.

В аппаратную среду изделий семейства «Криптофлэш» возможно встраивание сканеров папиллярных отпечатков пальцев человека, а в программы – соответствующих алгоритмов их обработки. Целью является внедрение в малогабаритные носители информации большой емкости со встроенными СКЗИ передовых технологий аутентификации и авторизации пользователей в соответствии с их биометрическими параметрами.

При подобном подходе может быть разработано и внедрено в практику устройство индивидуальной криптографической защиты информации пользователя, предназначенное для использования либо конкретным человеком, либо группой пользователей. При этом возможны режимы с генерацией личных сеансовых ключей пользователей из их биометрических параметров. При использовании подобной технологии исключается необходимость хранения и уничтожения ключей, как в среде СКЗИ, так и в среде, внешней по отношению к нему, включая ПЭВМ, т.к. носителем текущего ключа для доступа к информации является сам пользователь.

Это направление ФГУП «ПНИЭИ» рассматривает в качестве перспективного. На рисунке 4 приведены фотографии действующих опытных образцов, различающихся примененными сканерами отпечатков пальцев – соответственно с динамическим и статическим принципами действия.

ТЗ на разработку подобных изделий согласовано с в/ч 43753 для сертификации по классу КС1. При их разработке учтены положения отечественного ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации», разработанного с участием предприятия.

С помощью инфраструктуры УЦ [6] ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Однако, собственноручная подпись является индивидуальным биометрическим показателем человека, содержащим его тайный образ, а ЭЦП – результат совместной деятельности УЦ, выдающего сертификат на основе данных центра регистрации, и технических средств пользователя, осуществляющих работу с закрытым или открытым ключом ЭЦП [1]. В последнем случае имеет место «опосредованность» пользователя, чьи биометрические параметры анализируются только однократно в процессе первоначальной регистрации, как правило, на основе его регистрационных, учетных, паспортных и т.п.

В этой связи большую актуальность имеет задача внедрения биометрических параметров пользователя при формировании каждого электронного документа, а также их контроля при обращении или взаимодействии с УЦ, включая внедрение в сертификаты ключа подписи.

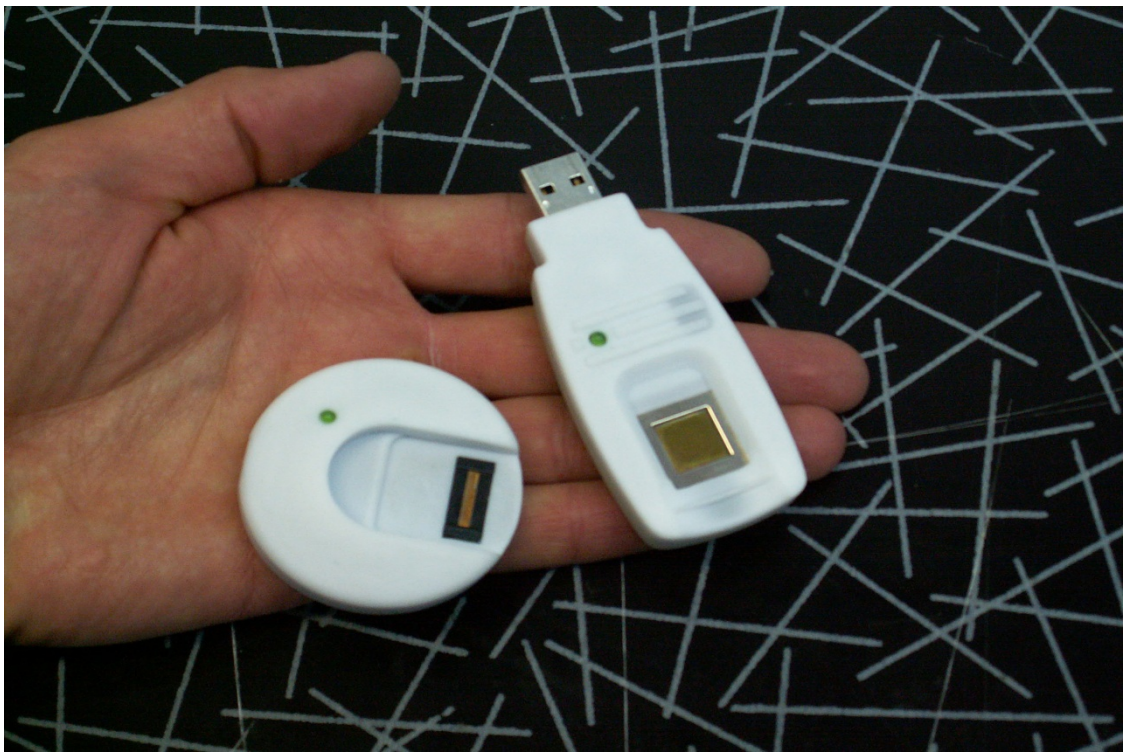


Рисунок 4

В этом случае может быть достигнута практически полная персонализация как всех действий при обращении к ресурсам ЭДО, так и электронных документов через индивидуальные биометрические параметры пользователей.

Одной из наиболее острых проблем формирования ЭЦП пользователей электронного документооборота, также требующая использования биометрических параметров пользователя, является надежная авторизация подписывающего. К сожалению, пользователи не редко передают друг другу свои полномочия. Например, пользователь может доверить формирование его ЭЦП своему подчиненному, набиравшему ранее документ на ПЭВМ. Привлечение менее квалифицированного пользователя для выполнение неквалифицированной работы следует приветствовать, но доверять кому либо формирование своей ЭЦП категорически нельзя. Надежная технология должна исключать такую возможность.

Для того, что бы существенно повысить уровень авторизации управления личными формирователями ЭЦП необходимо привлечение современных биометрических технологий высоконадежной аутентификации [6, 7]. Одна из таких технологий, построенная на анализе динамики рукописного почерка отражена на рисунке 5. Каждый из нас имеет уникальный рукописный почерк. На этом построена процедура подписывания автографом обычных бумажных документов. Исследования, проведенные в России и за рубежом показали, что наиболее удобен для автоматической идентификации человека анализ динамики «живой» рукописной надписи. При воспроизведении надписи осуществляется оцифровка колебаний пера X(t), Y(t) и давления пера на подложку Z(t). Эти оцифрованные данные являются биометрическим образом пользователя, используя несколько биометрических образов удается автоматически обучить искусственную нейронную сеть преобразовывать образ «Свой» в ключ формирования ЭЦП пользователя.

В ФГУП «ПНИЭИ» разработано программное обеспечение с использованием СКЗИ, разработанном ФГУП ПНИЭИ и находящемся на сертификации в ФСБ России, расширяющее функциональное назначение описанной выше технологии высоконадежной аутентификации пользователей.

Суть заключается в «воссоздании» ключевого контейнера СКЗИ из биометрических параметров пользователя (рисунок 5):

- после предоставления рукописного пароля на выходе нейросетевого преобразователя биометрии пользователя получается код безопасности;
- полученный в предыдущем блоке код безопасности, проходя через блок безопасных преобразований, «превращается» в ключевой контейнер пользователя СКЗИ;
- полученный ключевой контейнер используется СКЗИ для вычисления ЭЦП электронного документа.

Приведенные выше биометрико-криптографические механизмы высокоточной авторизации пользователей обеспечивают:

- работу с любым графическим планшетом, способным автоматически поддерживать режим эмулятора «мышь» в защищаемой вычислительной среде;

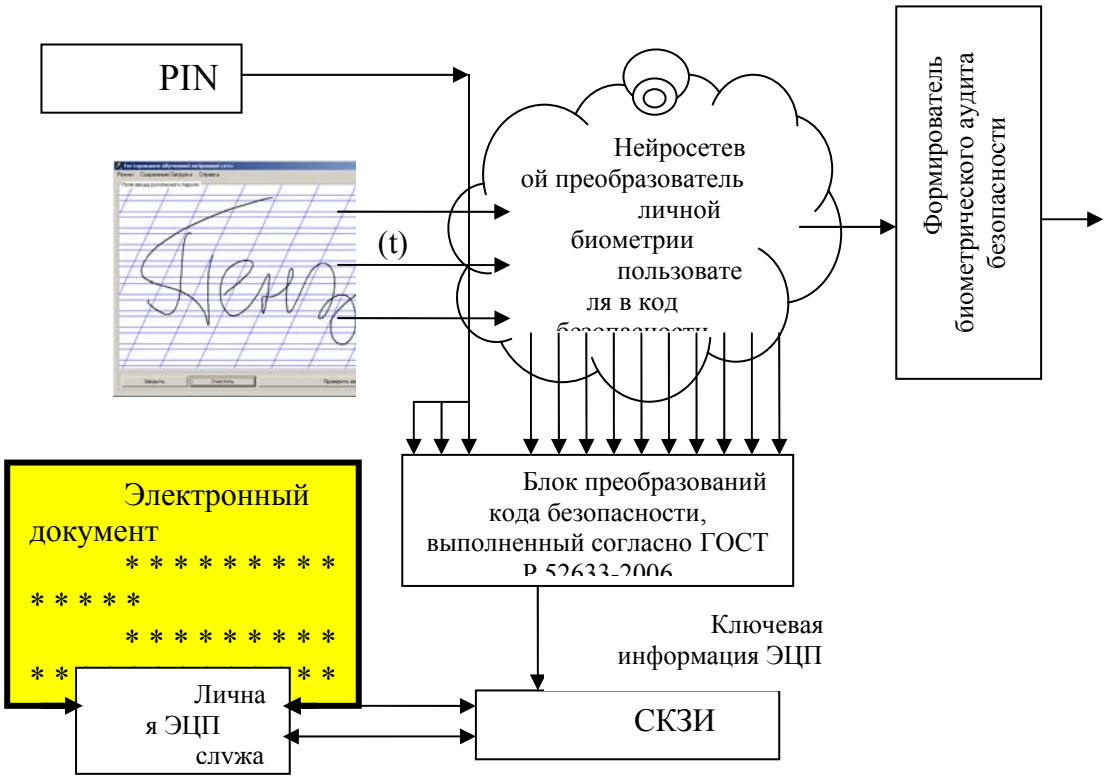


Рисунок 5 - Биометрико-нейросетевой криптоформирователь личной ЭЦП пользователя с высокой степенью авторизации

- автоматическое обучение нейросетевого преобразователя рукописных паролей в коды пароля доступа к ключевому контейнеру СКЗИ пользователя на 8 -:-16 примерах воспроизведения пользователем его рукописного пароля, за время обучения не более 30 секунд;
- работу с ключевым контейнером СКЗИ пользователя при обучении преобразователя биометрия-код;
- автоматическое тестирование стойкости преобразователя биометрия-код на примерах того или иного рукописного образа к атакам подбора злоумышленника не знающего рукописных паролей служащего;

- вероятность ошибки первого рода (ошибочный отказ в доступе «Своему») не более 0.3 при первой попытке воспроизведения рукописного пароля. Высокая доступность должны быть обеспечена разрешением до 11 попыток аутентификации. Вероятность ошибки первого рода при 11-той попытке аутентификации не более 0.00002.
- вероятность ошибки второго рода (ошибочный допуск «Чужого» под логином «Своего» к ключевому контейнеру СКЗИ «Своего») для среднестатистического пользователя (для рукописного пароля в одно слово-5 букв) не должна быть более 0.0000000000000001 (десять в минус 16 степени) при сохранении пользователем двух рукописных паролей (доступа к АРМ и доступа к ключу ЭЦП) в тайне.
- дообучение и переобучение хранителя ключевого контейнера СКЗИ пользователя должно осуществляться только после его предварительной биометрической аутентификации, никто кроме самого пользователя не может изменить его пароль доступа к ключевому контейнеру СКЗИ.

В комплексе, по мнению ФГУП «ПНИЭИ», описанные технические решения и механизмы биометрико-криптографической аутентификации позволят внедрить в интегрированной сети с электронным документооборотом новые принципы реализации дифференцированной политики безопасности с юридически значимой ЭЦП с максимальным использованием автоматизированных процессов управления и дистанционного мониторинга.

ЛИТЕРАТУРА:

6. ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
7. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая».
8. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хеширования».
9. Отчеты НИР, ОКР.
10. Федеральный Закон «Об электронной цифровой подписи» от 10.01.2002 года №1-ФЗ.
11. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.
12. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
13. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Изд-во Пензенского гос. ун-та, 2000. – 188 с.

Получено 12.11.2006 г. Опубликована в Интернет 13.11.2006.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С37-39... Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/009)

ОЦЕНКА ФРАКТАЛЬНОСТИ НЕЙРОСЕТЕВЫХ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ-КОД ПРИ ВЫСОКИХ ВХОДНЫХ РАЗМЕРНОСТЯХ ДАННЫХ

Иванов А.И., Надев Д.Н., Захаров О.С., Агеев М.Е., Хозин Ю.В., Капитуров Н.В.

ФГУП «Пензенский научно-исследовательский
электротехнический институт»

Выполнение требований отечественного стандарта [1], позволяет создавать высоконадежные преобразователи биометрия-код и использовать их как контейнеры для хранения криптографического ключа пользователя и его конфиденциального биометрического образа [2]. Естественно, что эта новая технология нуждается в тестировании. Возможно несколько подходов к тестированию биометрико-нейросетевых контейнеров [3]. Одним из таких подходов является искусственное ослабление биометрико-нейросетевой защиты. При тестировании защиты мы знаем сам биометрический образ пользователя (имеем 10-:-16 примеров его реализации). Как следствие мы можем подбирать не все входные биометрические данные, а только их часть. Это ускоряет численный эксперимент, который реализуется путем создания специальной тестирующей машины.

Тестовая машина использует знание о том, что входные биометрические параметры имеют нормальный закон распределения значений. Кроме того, предполагается, что злоумышленник, атакующий биометрию, знает наиболее вероятное значение дисперсии всех входных данных множества «Все Чужие».

Тестовая машина строится таким образом, что бы подбирать часть неизвестных входных параметров. Чем больше входных биометрических параметров подбирается, тем больше времени уходит на их подбор. Соответствующий график логарифма числа попыток подбора как функция числа подбираемых входов нейросети отображен на рисунке 1. На подбор тестовой машиной 90 биометрических параметров уходит примерно 10 минут машинного времени. Если пытаться подбирать 120 биометрических параметров время тестовых испытаний составит 1 час при тестировании биометрической защиты на Pentium 4 (3 GHz, ОЗУ 512 Мбайт). Подбор всех 416 входов биометрического преобразователя будет занимать около 2000 лет, однако реальная атака подбора должна занимать примерно 21 год. Дело в том, что атакующие машины работают примерно в сто раз быстрее тестовых (атакующие и тестовые машины создаются под разные цели). Тестовые машины вынуждены повторять подбор некоторого случайного сочетания входных данных по 100 раз для последующего усреднения конечного результата. Атакующие машины перебирают данные без повторений и потому оказываются примерно с 100 раз быстрее тестовых машин.

Получается, что пользователь, сохраняющий в тайне свой биометрический пароль “*Пенза”* (см. рисунок 1), имеет в своем распоряжении преобразователь биометрия-код со стойкостью к атакам подбора порядка $10^{15,8}$. Такая стойкость эквивалентна использованию ключа симметричного криптографического преобразования длинной 52 -:- 53 бита (более точно 52,486 бита) Биометрико-нейросетевой защиты такой стойкости к атакам подбора вполне достаточно для многих практических приложений.

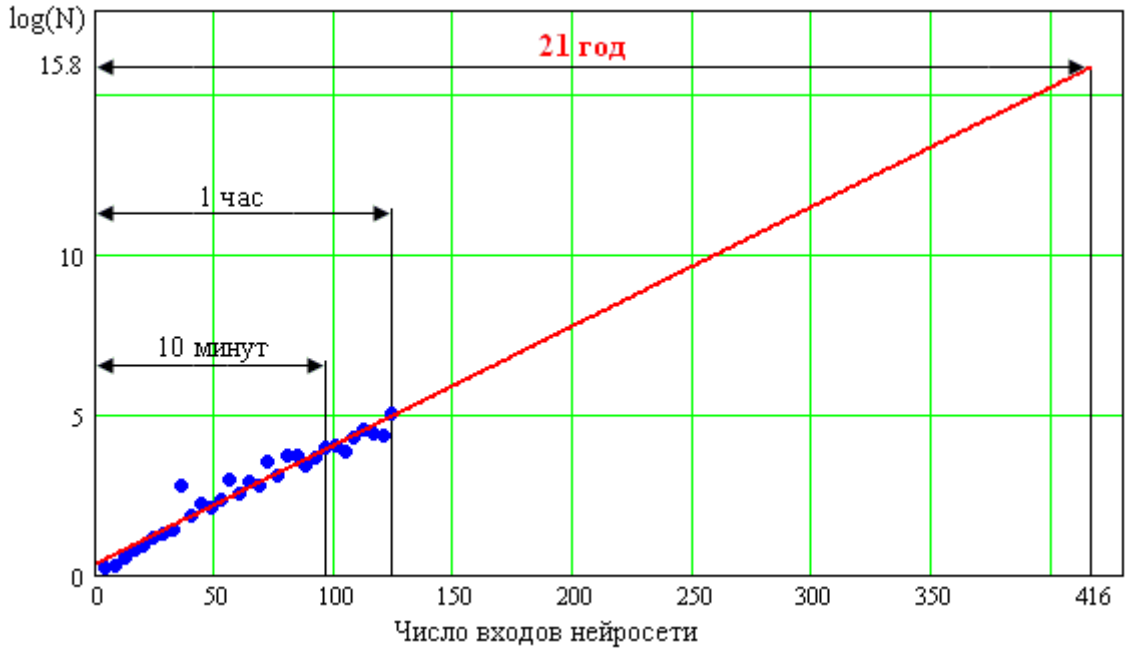


Рис. 1. Численный эксперимент по достоверной оценке стойкости нейросетевого хранителя конфиденциальной биометрико-криптографической информации.

Заметим, что по горизонтальной оси графика рисунка 1 отложено число входов или длина идеального биометрического ключа. Если бы биометрические данные были независимы, мы получили бы идеальный ключ длинной 416 бит. В место этого мы имеем идеальный ключ с дробной (фрактальной) длинной 52,486. Одним из признаков самоподобных статистических фракталов является их описание линейной функцией в логарифмических координатах [4]. Обе координаты графика рисунка 1 являются логарифмическими. Соответственно наклон прямой этого графика является показателем фрактальности тестируемого преобразователя биометрия-код.

В рассматриваемом нами случае дробная (фрактальная) длинна ключа оказывается связана с числом биометрических входов соотношением:

$$k = a \cdot N \quad \text{или} \quad k = 0{,}126 \cdot N \qquad (1),$$

где k – дробная (фрактальная) длина биометрического ключа;

a = 0,126 – показатель фрактальности (константа);

N – число входных биометрических данных.

Видимо для биометрических систем показатель фрактальности всегда будет меньше единицы, в то время как для классических фракталов он оказывается больше единицы [4]. Это связано с сильными корреляционными связями, присутсвующими в биометрических данных.

Следует подчеркнуть, что каждый из биометрических входов имеет разное качество и в этом контексте трудно говорить о «самоподобии» статистических фракталов [4] реальных биометрических данных. Однако после перемешивания групп тестируемых входов и после усреднения результатов их тестирования «самоподобие» все же проявляется. Как видно из рисунка 1 экспериментальные данные хорошо описываются линией.

Дробная (фрактальная) размерность биометрических ключей, не позволяет использовать для описания атак подбора биометрических данных хорошо изученные тактики организации атак подбора ключей с классической, целой

размерностью. На данный момент неизвестны хорошо спланированные эффективные атаки подбора параметров неизвестного биометрического образа высокой размерности.

Одним из интересных топологических моментов является то, что у преобразователей биометрия-код фрактальная размерность ключа может быть определена как по входу (1), так и по выходу. График рисунка 1 соответствует преобразователю биометрия-код с 416 входами и 256 выходами. Очевидно, что для выходных данных преобразователя мы также можем вычислить показатель фрактальности и записать аналог уравнения (1). При этом показатель фрактальности оказывается уже не константой, а функцией:

$$k = a(N) \cdot N \qquad (2).$$

Предположительно для идеальных преобразователей биометрия-код функция a(N) будет по прежнему константой, которая существенно выше фрактальной константы входных биометрических данных. Однако для реальных нейросетевых преобразователей биометрия код сделать все парные связи нейросети некоррелированными не удается. Из-за этого увеличение числа нейронов в преобразователе (увеличение числа выходов у нейронной сети) не приводит к линейному росту качества принимаемых решений [5] при сохранении того же числа входов нейросети.

Функция a(N) для биометрических систем при малых значениях N имеет большое значение, близкое к значению показателя фрактальности идеального преобразователя биометрия код. Однако с ростом N значения функции a(N) падает, что эквивалентно наличию некоторого барьера конечной информативности используемого биометрического образа.

Получается, что из-за некоторых технических ограничений [5] показатель фрактальности из константы превращается в функцию. Это эквивалентно вырождению симметричных самоподобных фракталов в некоторые более слабые фрактальные (функции) преобразования. Входные биометрические данные являются действительно фрактальными, а вот выходные данные преобразователя биометрия-код теряют свою фрактальность с ростом размерности.

ЛИТЕРАТУРА:

1. ГОСТ Р 53633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
2. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.
3. Малыгин А.Ю., Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации /Пенза-2006 г., Издательство Пензенского государственного университета., 161 с.
4. Кроновер Р. Фракталы и хаос в динамических системах. М: Техносфера- 2006, 488 с.
5. Захаров О. С., Иванов А.И., Хозин Ю. В. Невозможность практической реализации нейросетевого «информационного» вечного двигателя с неограниченно большим числом выходов. «Нейрокомпьютеры: разработка, применение» № 7 2007 г.

Получено 10.03.2007 г. Опубликована в Интернет 19.04.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С.40-11. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v08/010)

ЗАЩИТА ОТ ПОПЫТОК ИССЛЕДОВАНИЯ ИСПОЛНЯЕМЫХ ПРОГРАММ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПРИ ЗАХВАТЕ ИХ ПРОТИВНИКОМ

Майоров А.В., Иванов А.И., Шашков Б.Д.

Лаборатория биометрических и нейросетевых технологий Пензенского научно-исследовательского электротехнического института

В соответствии с ГОСТ Р 52633-2006 определены требования к высоконадежным средствам биометрической аутентификации пользователя. При выполнении требований ГОСТ Р 52633-2006 нейросетевой преобразователь биометрия-код позволяет сокрыть биометрические данные пользователя и его личный криптографический ключ. Извлечь конфиденциальную информацию из параметров связей нейросетевого преобразователя сложно, что и является определенной защитой исполняемых программ. У нового класса программ появилось интересное свойство: исполняемый код нейросетевого преобразователя оказывается защищенным от исследования, оставаясь исполняемым.

Заметим, что обычный исполняемый код может быть гарантированно защищен от исследования, например, его шифрованием [2]. Однако этот прием технический прием нежелателен для применения, так как перед исполнением программы ее исполняемый код должен быть расшифрован. То есть в той же самой программе должен находиться ключ расшифрования программы, что недопустимо [3]. Желательно гарантированно защищать программы от исследования, сохраняя их исполняемость.

Как было отмечено выше, нейросетевые технологии позволяют скрывать конфиденциальную информацию, однако нейросетевые технологии должны быть обрамлены классическими обслуживающими их программами. Эти классические обслуживающие программы должны быть выполнены специальным образом, так что бы гарантированно исключить их изучение вне режима «АВТОРИЗОВАННОГО» исполнения [2-3].

В качестве примера рассмотрим программный нейросетевой хранитель длинного случайного пароля пользователя, обученный преобразовывать биометрический образ «Свой» в этот пароль. Длина пароля, его содержание могут быть произвольными. Например, работа программного хранителя пароля в ОС Windows Mobile 5.0 может быть до 29 символов. Очевидно, что длина пароля должна учитываться при обучении преобразователя биометрия-код и храниться в программе. Длина пароля является конфиденциальной информацией пользователя. Необходимо, чтобы программное обслуживающее обеспечение гарантированно скрывало длину пароля пользователя.

Например, нейросетевой преобразователь биометрия-код формирует на выходе пароль длины до 256 бит для рукописного входного образа «Свой» из 5 букв. В случае задания пароля меньшей длины, оставшиеся выходы нейросети должны давать случайные коды для исключения компрометации длины пароля. Таким образом, для обучения нейросетевого преобразователя, формируется код K = P+N, где P – пароль пользователя длиной L, N – шум, дополняющий

защищаемый пароль до 256 бит. В простейшем случае первые L бит кода N должны быть нулевыми.

Для того, чтобы скрыть информацию о длине L пароля пользователя, он представляется как сумма двух величин C и H_M, где C – число-дополнение, а H_M – значение хеш-функции, зависящее от выходного полного кода K, вырабатываемого нейросетевым преобразователем биометрия-код. В программе вместо длины пароля хранится число-дополнение C, только по одному значение которого длина пароля не может быть восстановлена. На этапе обучения нейросетевого преобразователя значение числа-дополнения C вычисляется как $C = L - H_M$ и сохраняется в программе.

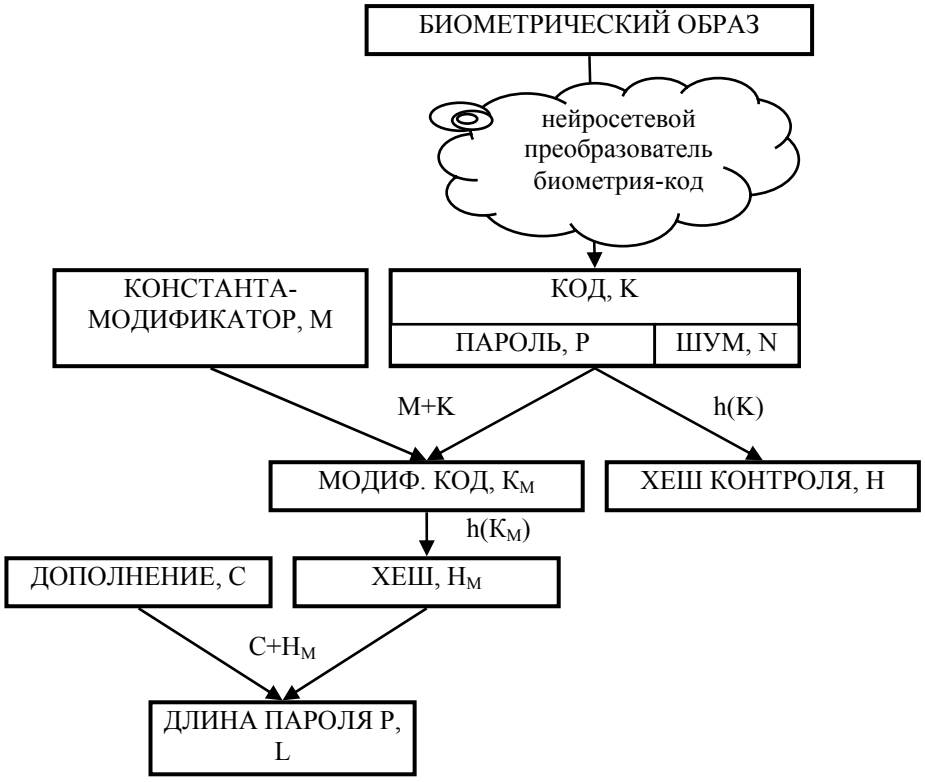


Рисунок 1. Диаграмма преобразования данных в исполняемом модуле с гарантированной защитой от исследования

На рисунке 1 показана диаграмма преобразования данных, используемых в процессе извлечения хранимого пароля пользователя из обученной нейронной сети.

Нейросетевой преобразователь, получая на вход биометрические данные пользователя, на выходе выдает некоторый код K. После этого проводится авторизация пользователя при помощи сравнения значения вычисленной хеш-функции h(K) с ее эталоном, полученным во время обучения нейронного преобразователя биометрия-код. В случае совпадения значений хеш-функции и эталона, режим выполнения программы является авторизованным, выходной код является верным, первые L его разрядов соответствуют паролю пользователя.

Для определения L строится модифицированный код K_M и вычисляется значение хеш-функции $H_M = h(K_M)$. Модификация выходного кода нейросети (преобразование K в K_M) осуществляется любой однозначной функцией, например, путем сложения с константой открыто хранящейся в программе. Длина пароля пользователя P рассчитывается по формуле $L = H_M + C$.

Представленное решение может успешно использоваться для сокрытия значения любого числа управляющих данных биометрической защиты. Использование числа-дополнения, длиной 128 бит, и хеш-функции MD5 позволяет надежно скрыть малые секреты длиной до 128 бит.

Вторая проблема работы с маленькими секретами заключается в безопасном размножении числа малой длины до числа большой длины. Возможным решением может стать использование заполнителя длинного числа хеш функциями от исходного числа. В первый блок длинного числа помещается исходное число, малой длины. Во второй – значение хеш-функции от первого блока, т.е. от P_0. В третий – значение хеш-функции от первых двух блоков, т.е. от числа $[P_0..P_1]$ и т.д. Однако, оно не является лучшим в силу потери значащих бит исходного ключа в ходе операции вычисления хеш-функции. Кроме этого, данное решение является неприменимым для массовых операций размножения в силу больших временных затрат.

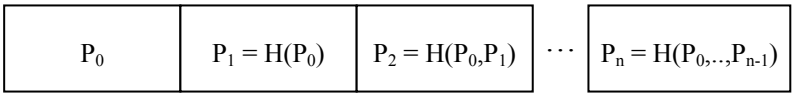


Рисунок 2. Операция размножения малого секрета при помощи хеш-функции

Более удачным является вариант с использованием правых или левых циклических сдвигов исходного малого числа P_0. В этом случае, в соответствии с рисунком 3, исходного значение последовательно сдвигается на 1,2,...,n разрядов добавляется в следующую область памяти длинного числа. Например, для размножения 256-битного числа до 1024-битного достаточно 3 операции циклического сдвига. Максимальная длина числа, которое может получиться из короткого n-битного равна n^2 битам. Исходное число P сохраняется в длинном числе первым. Обратная операция выполняется обрезанием длинного числа до нужной длины.

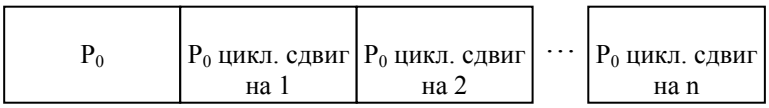


Рисунок 3. Операция размножения малого числа через сдвиг

Предложенный выше подход к защите исполняемого кода программы выгоднее шифрования того же исполняемого кода, так как:

- в программе нет ключа расшифрования;
- шифрование заменено хешированием;
- сокращается код, ускоряются вычисления;
- появляется возможность маскирования факта сокрытия управляющего параметра, если число хеш-функций больше числа скрываемых управляющих параметров.

ЛИТЕРАТУРА:

1. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации»
2. Fritz Hohl , «Time Limited Blackbox Security: Protecting Mobile Agents From Malicious Hosts», 1998
3. Tomas Sander, Christian F. Tschudin. «Protecting Mobile Agents Against Malicious Hosts», 1998

Получено 20.03.2007 г. Опубликована в Интернет 19.04.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С…43-45... Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/011)

ПРОТИВОДЕЙСТВИЕ УГРОЗЕ МАССОВОГО ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКОЙ «ПЕЧАТИ ЗВЕРЯ»

Иванов А.И.

> *«И поклонились зверю, говоря: кто подобен зверю сему и кто может сравниться с ним.» (Апокалипсис 13:4)*
>
> *«И он сделал то, что всем – малым и великим, богатым и нищим, свободным и рабам – положено будет начертание на правую руку или на чело их, и что никому нельзя будет ни покупать, ни продавать, кроме того, кто имеет это начертание, или имя зверя, или число имени его. .... …….это число человеческое; число его шестьсот шестьдесят шесть» (Апокалипсис 13:16-18).*

Терроризм по своей сути является отражением неустойчивости общества. По мере информатизации современного общества его неустойчивость возрастает. Сегодня террористы, обладая незначительными материальными и людскими ресурсами способны оказать существенное влияние на политические решения стран со значительными духовными, материальными, людскими ресурсами. Предстоящий вывод войск большого брата из Ирака – пример того, когда одна из сторон прибегая к тактике террора фактически одерживает военную победу малой кровью и малыми ресурсами. Современный террор фактически является атакой на массовое сознание страны противника через его же средства массовой информации. Ввод военного положения для всех средств массовой информации – в форме военной цензуры (без введения военного положения как такового для населения) сводит на нет информационный терроризм.

Заметим, что устойчивость любого общества имеет явную связи с реализуемыми в нем политиками учетности (ресурсов, людей, информации). Устойчивое общество имеет адекватную политику учетности и как только политика учетности отстает от потребностей, общество становится неустойчивым.

Одним из механизмов осуществления политики учетности материальных ресурсов страны являются деньги. Подделка денежных знаков – это атака на государственный механизм учетности материальных ресурсов.

Еще одним механизмом учетности людей являются паспорта. Подделка паспорта или проведение операции под «Чужим» паспортом является атакой на механизм государственного учета людей.

Современные технологии сделали доступным средства копирования паспортов и денег широкому кругу лиц. В связи с этим ведущие государства стремятся восстановить ослабление своих политик учетности. Ими вводится новое

поколение паспортно-визовых документов с биометрической автоматизированной идентификацией человека, активно модифицируются полиграфические технологии изготовления бланков документов и банкнот. Государства пытаются усилить политику учетности пологая, что хаосу нестабильности может быть противопоставлена только политика повышения уровня учетности информации, материальных ресурсов, людей.

Современная криптография активно создает механизмы учетности и авторизации такие как то: электронная цифровая подпись, цифровые водяные знаки,… Видимо в ближайшее время политику учетности можно будет поднять на значительно более высокий уровень так как появились новые технологии (малогабаритные, перепрограммируемые микросхемы учетности с низкой стоимостью, большой памятью и бесконтактным высокоскоростным радионтерфейсом обмена данными [1]).

Вопрос уже не стоит о том, как и где будут использоваться Memory Spot, вопрос стоит о том, чем бы будем заполнять мегабайты памяти этих микросхем. К сожалению, в этом контексте следует констатировать тот факт, что большой брат за океаном и братья поменьше из НАТО идут только по пути создания цифровой диктатуры. В период с 2000 по 2007 г. г. за пределами России было принято порядка 56 международных и национальных биометрических стандарта и все эти стандарты относятся к полицейским. Все они направлены на контроль людей, предусматривают практически открытое (слабо защищенное) использование открытых биометрических образов людей (отпечатков пальцев, радужной оболочки глаз, геометрии лица,..). Усилиями большого брата и стран НАТО фактически реализуются предсказанная в Апокалипсисе ситуация (смотри эпиграфы перед статьей). Если у всех людей снять биометрию, и дать задокументировать ее зверю, то мы фактически получим «печать зверя». В Апокалипсисе описана предельная ситуация полной учетности людей зверем, причем на недобровольной основе. Интуитивно понятно, что неоправданное усиление политик учетности не менее опасно для стабильности общества, как и их ослабление.

Следует особо подчеркнуть, что единственной страной которой дано глубокое понимание затронутых выше проблем является Россия. Россия является единственной страной, которая развивает технологии цифровой биометрической демократии. С 1 апреля 2007 года у нас вступил в действие национальный стандарт [2], который фактически снял проблему «печати зверя».

Россия своим новым стандартом дала миру общегражданские технологии обеспечивающие анонимность биометрии, возможность при необходимости поменять свой биометрический образ, возможность каждому не только быть надежно проверенным, но и самому проверять других и убедиться, что тебя

проверяет твое государство, а не кто попало (например, некое преступное сообщество).

Кажется странным, что это все сделала Россия, а не запад, который кичится правами человека и демократией. На самом деле западный взгляд на цифровую демократию, точно повторяет взгляды большого брата, а последние вообще не является демократией. Примером могут служить их технологии голосования. По этим технологиям голосуют не люд, а ключи на смарт-картах. Обычные люди не способны надежно хранить свои секретные ключи [3], то есть существует реальная возможность того, что тот, кто генерирует и хранит ключи, сможет проголосовать за кого угодно. Перефразируя Сталина можно утверждать: не важно кто как голосует и кто как считает голоса, важно кто готовит криптографические ключи для будущего голосования.

Для стран НАТО и США демократия – это не более чем повод оказывать на всех остальных политическое давление. Эпоха их крестовых походов у них сменилась на следующую эпоху гуманитарных войн и гуманитарных бомбардировок.

Только введенный в нашей стране национальный стандарт [2] открывает реальную возможность резкого повышения уровня учетности материальных ценностей (в виде электронных денег) и людей, через их электронные паспорта. Так как это стандарт выгоден людям и безопасен для них, он, видимо, будет принят гражданским обществом. Высока вероятность того, что люди не будут отторгать нововведение, позволяющее им отказаться от запоминания множества паролей, ПИН кодов, ключей доступа. При использовании нового стандарта криптография перестает отторгаться обществом и сможет реально защитить интересы обычных граждан. Теперь каждый из нас при желании может выйти из под контроля тех, кто хранит наши ключи или живет за наш счет, делая вид, что хранит наши ключи и их сертификаты.

Литература:

1. Сергей Асмаков Технология Memory Spot. КомпьютерПресс № 1, 2007 г.
2. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации»
3. Иванов А.И., Анисимова Л.Ю., Акмаев А.А. Механизмы противодействия «цифровому неравенству» граждан информационного общества /Защита информации INSIDE. № 4, 2006, с. 26-29.

Получено 20.05.2007 г. Опубликована в Интернет 13.06.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С…45-54... Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/012)

ПОЛИТИКА ФОРМИРОВАНИЯ РЫНКА ВЫСОКОНАДЕЖНЫХ СРЕДСТВ БИОМЕТРИЧЕСКОЙ АВТОРИЗАЦИИ

Анисимова Л.Ю.

Рынок

Рыночные преобразования поставили российских производителей перед проблемой адаптации к качественно новым макроэкономическим условиям.

При формировании рынка предприятия, оперирующие на стабильном рынке, в отраслях, не подверженных быстрым переменам, как правило, боролись за увеличение своей доли рынка. Емкость же рынков возрастала вместе с ростом численности населения. Классической рыночной стратегией фирмы здесь было увеличение своей доли на намеченном рынке за счет снижения цен и издержек производства своей продукции. Доля рынка, контролируемого данной фирмой, в этих условиях, конечно, не могла быть очень большой, отчасти в силу правительственных мер антимонопольного регулирования экономики.

В современном быстроменяющемся мире рыночная конкуренция становится все более жесткой. Чтобы не только существовать, но и расширять свой бизнес, компании в современных условиях должны исповедовать концепцию интегрированного маркетинга, который ориентирован на ПРЕДВОСХИЩЕНИЕ нужд и запросов потребителей.

В информационную эру, когда новые нужды и запросы потребителей быстро распространяются по всему свету и в то же время становятся чрезвычайно индивидуализированными, когда рынки становятся разнообразными по своей структуре, руководство компании, если оно стремится к преуспеванию на рынке, должно неукоснительно следовать правилу: **делать, прежде всего, ставку на продукты, генерирующие реальные денежные поступления**.

Никогда ранее компании не оказывались в такой ситуации, как сейчас. Все рынки разделены на множество сегментов. Специализация достигла такого уровня, что от конкуренции можно еще укрыться разве что **на небольшом пространстве между двумя смежными сегментами различных рынков или одного и того же рынка.**

В наиболее передовых отраслях промышленности (например, в электронной) жизненный цикл изделий постоянно сокращается. Если в 80-х годах замена технологий происходила сначала через 10 лет, а затем через 5 и 2 года. То сейчас ведущие японские фирмы "выбрасывают" на рынок новые виды микросхем (основу любой радиоэлектронной аппаратуры потребительского и производственного назначения) в среднем каждые три месяца. Вспомните, когда появились и как быстро исчезли с рынка персональные компьютеры с 386-м процессором? В течение двух лет. Сегодня их в продаже и не найти [5].

Для достижения успеха на рынке главным сегодня является способность фирмы ранее других, или, по крайней мере, в момент имеющейся потребности, предоставить потребителю товар более высокого качества, чем прежде, или обладающего какими-то новыми свойствами, чем ранее, и притом за ту же или меньшую цену.

Для этого нужно отчетливо представлять себе, в чем именно состоят преимущества компании на рынке, в чем заключается его так называемая

"ключевая компетентность", что она умеет делать лучше всех производителей, представленных на рынке.

В рамках данной статьи рассматривается ситуация на рынке биометрических средств.

Этот рынок существует не первый год. Но наиболее бурное развитие рынок биометрических продуктов получил в последнем десятилетии. На сегодняшний день существуют тысячи фирм, создающих и продающих биометрические продукты. Наиболее наглядно общие тенденции в развитии рынка биометрических решений можно проиллюстрировать на примере стремительного роста объема рынка биометрических технологий после 11.09.2001. По прогнозу аналитической группы Allied Business Intelligence, сделанному в 2000 г., т.е. до террористического акта в Нью-Йорке, объем данного рынка в 2003 г. должен был составить $153млн. Реальные цифры составили $719млн. Интересны исследования и прогнозы консалтинговой компании International Biometric Group (IBG), специализирующейся на исследованиях в области биометрии. Долгосрочный прогноз IBG, которая до сих пор являлась наиболее объективной, показывает, что к 2008г. оборот биометрических компаний достигнет $4639млн. Динамика роста объема рынка биометрии на период 2004-2008гг. по прогнозу IBG представлена на рис.1.

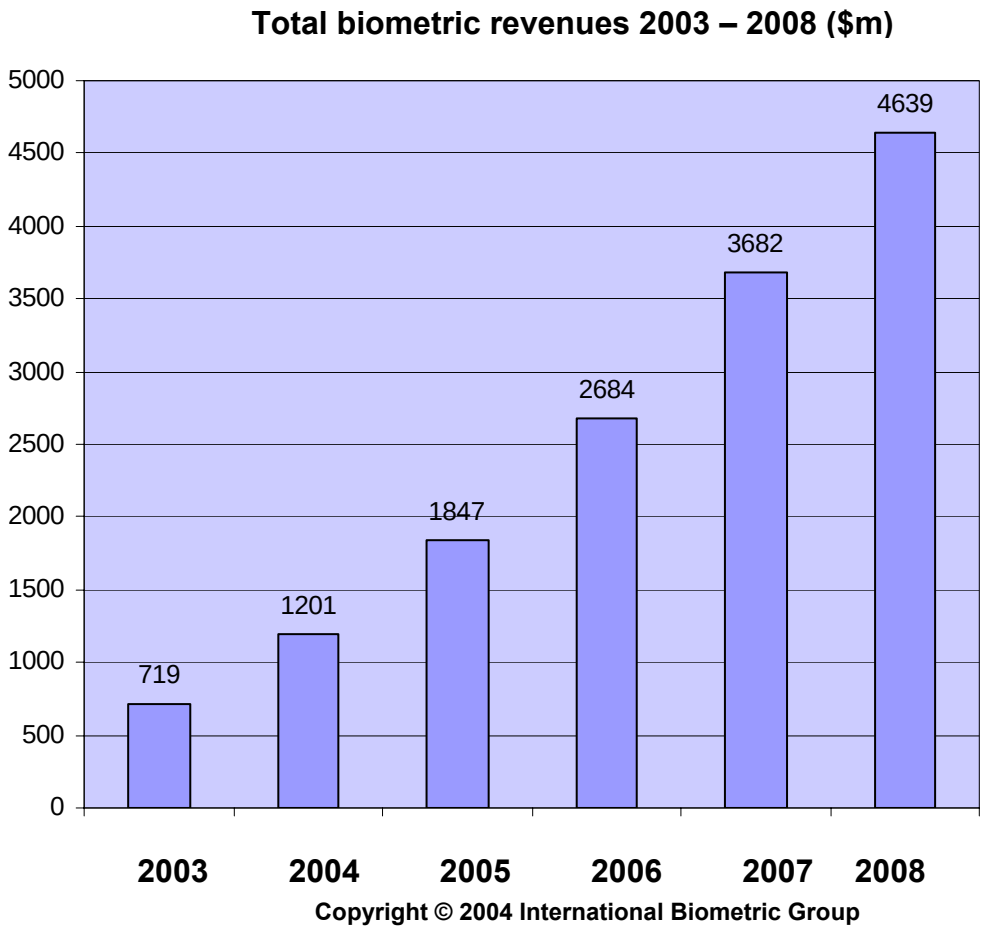


Рисунок 1 – Показатели развития рынка биометрических технологий

Таким образом, рынок биометрических технологий и оборудования на сегодняшний день является одним из наиболее активно развивающихся сегментов рынка информационных технологий, прогнозируемые темпы роста составляют порядка 40%.

Формирование нового сегмента рынка

Вполне естественно, что на первых порах развитие биометрии было хаотичным, продукты, предлагаемые на этом рынке, имели ряд существенных недостатков. Не могло быть и речи о совместимости интерфейсов конкурирующих фирм или о добровольном открытии ими своих программных кодов, методик обработки и особенностей первичных преобразований информации с физического уровня в цифровую форму. Однако развитие технологии постепенно поставило ВСЕХ производителей перед осознанием преимущества объединения усилий и стандартизации продукции. Лидером в этом отношении стали Соединенные Штаты Америки.

Соединенные Штаты на данный момент смогли дальше всех пройти по пути национальной стандартизации биометрических устройств и технологий. На данный момент в США и странах западной Европы выпущено порядка 55 национальных и международных биометрических стандартов. В этой работе задействованы национальные институты стандартизации США NIST (National Institute of Standards and Technology) и ANSI (American National Standart Institute). Готовятся к введению порядка 30 новых документов, регламентирующих разработку и использование биометрических продуктов и технологий [4]. Таким образом, США приложили огромные усилия и направили огромные денежные ассигнования на формирование рынка биометрических средств и технологий «под себя» и теперь получают отдачу от своих вложений, продвигая свои технологические наработки 1996-2002 гг.

Однако следует учесть, что биометрия, предлагаемая зарубежными компаниями, имеет непозволительно низкий уровень критичных параметров, и ориентирована на решение полицейских задач контроля населения.

В таблице 1 приведены результаты сравнения новых российских биометрических технологий и зарубежных биометрических технологий первого поколения.

Таблица 1

Параметр сравнения	Первое поколение биометрических технологий	Второе поколение биометрических технологий (разработка России, г. Пенза 2002-2005 гг.)
Вероятность ошибки	10^{-2}, …., 10^{-4}	10^{-12}, ….., 10^{-22}
Использование в Internet и других открытых системах	Невозможно	Возможно
Использование при голосовании	Невозможно	Возможно
Использование в электронном документообороте	Невозможно	Возможно
Использование в Internet банках	Невозможно	Возможно

Безопасное объединение с криптографией	Невозможно	Возможно
Использование государством для проверок граждан	Возможно	Возможно
Использование гражданами для взаимных проверок	Невозможно	Возможно
Сохранение конфиденциальности биометрии граждан	Невозможно	Возможно
Обеспечение анонимности	Невозможно	Возможно

Значительное улучшение критичных характеристик биометрических продуктов российских производителей обеспечивается тем, что наряду с биометрией, обеспечивающей идентификацию пользователя, введено нейросетевое преобразование биометрического образа в код криптографического ключа, что значительно повышает надежность разрабатываемых продуктов и технологий.

ВЫВОД 1. Таким образом, намечен новый сегмент рынка (который на основе прогноза может перерасти в самостоятельный рынок) на стыке рынка биометрических продуктов и рынка средств криптографической защиты информации - криптографические средства защиты информации на основе биометрико-нейросетевых технологий. Лидером этого сегмента на сегодняшний день является Россия (Пенза, ФГУП "ПНИЭИ"), как изготовитель первых образцов высоконадежных биометрических средств защиты информации и разработчик ГОСТ 52633-2006 [1].

Стандартизация

Далее для легитимного присутствия в этом сегменте рынка России требуется в срочном порядке направить свои усилия на стандартизацию разрабатываемых биометрических продуктов (с перспективой выхода на международный рынок).

ВЫВОД 2. Чтобы выйти на международный рынок Россия должна применить приблизительно ту же **схему «прорыва» в части стандартизации разработки биометрических средств,** как и США (см. рисунок 2).

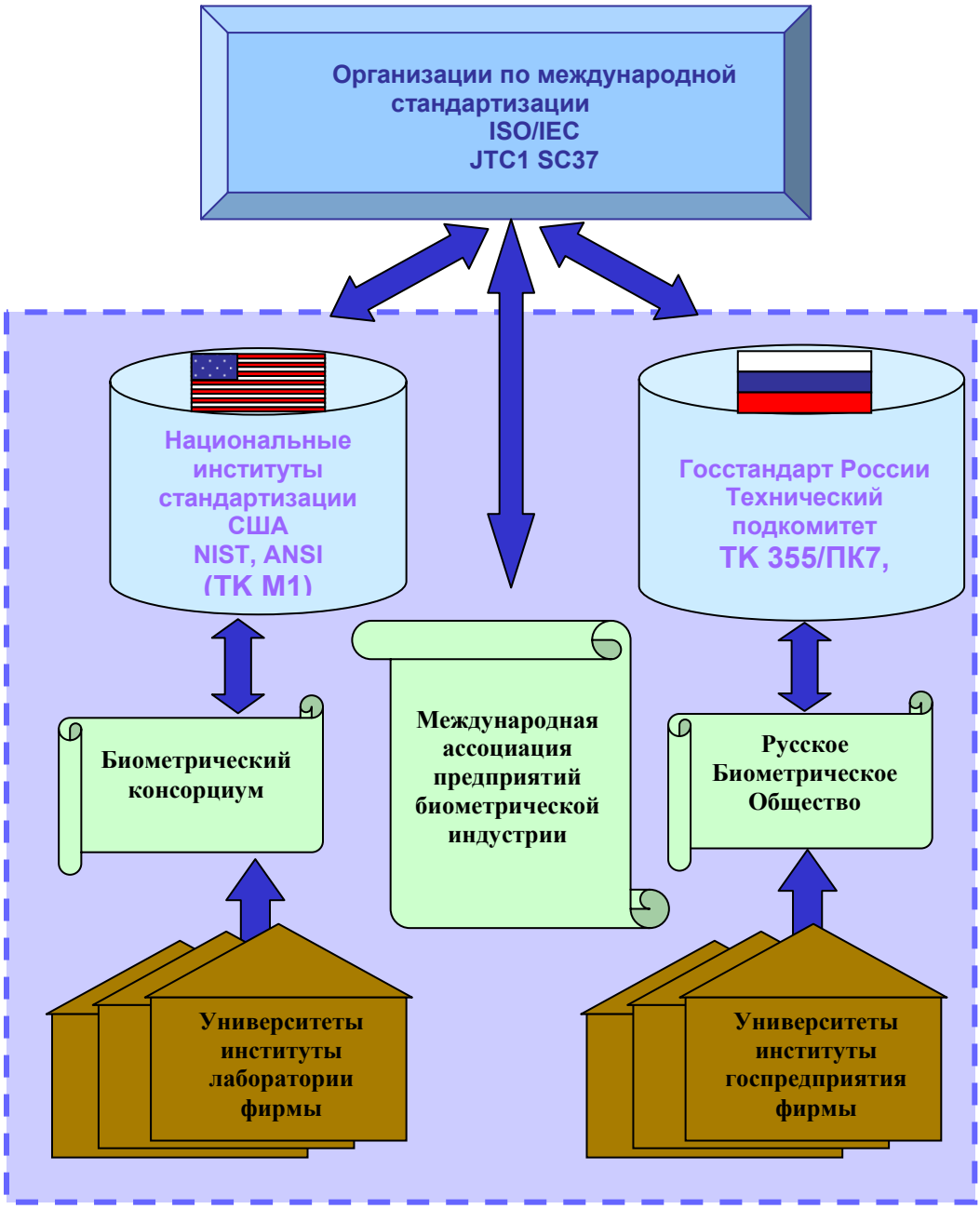


Рис. 2 – Структура технологии государственной стандартизации разработок в области биометрии

Первые шаги уже сделаны. В настоящее время в России формируется номенклатура национальных биометрических стандартов, подлежащих первоочередной разработке. Происходит формирование национальной технической политики по отношению к существующим и перспективным биометрическим технологиям.

Ведущую роль в этих процессах играет Госстандарт РФ.

Уже сегодня введен в действие стандарт по ВЫСОКОНАДЕЖНОЙ биометрии [1]. В течение 2008-2009 гг. планируется разработка еще двух стандартов – по формированию тестовых баз биометрических образов и по тестированию разрабатываемых биометрико-криптографических средств защиты информации.

Перспективы рынка высоконадежных биометрических средств

Растущий интерес к биометрическим системам и технологиям способствует тому, что эта отрасль на мировом рынке активно развивается.

Преимущества данных продуктов выглядят очень привлекательными и данные технологии занимают свое место в системах безопасности. Некоторые из лучших на сегодня биометрических систем помогают компаниям и предприятиям сохранять время и деньги, обеспечивая высокий уровень безопасности.

Кроме того, на сегодняшний день биометрические технологии появляются и в школах, и в госпиталях, и в аэропортах.

Уровень развития биометрических технологий в России и востребованность отечественных разработок в этой области на мировом рынке свидетельствуют о высоком потенциале российской биометрии.

В то же время задачи биометрии, соответствующие российским масштабам, назрели и необходимость их решения стала актуальной. К таким задачам относятся:

- унификация и стандартизация биометрических систем и технологий;
- отработка и реализация методик оценки эффективности систем и алгоритмов распознавания;
- создание экспортно-оринетированного потенциала российской биометрии как одной из высокотехнологических отраслей;
- координация отраслевых и федеральных программ в области биометрии.

Безусловно, часть секторов на этом рынке нами уже безвозвратно потеряны, но есть еще не мало незанятых сегментов. Особенно с точки зрения секторов, находящихся на стыке различных сегментов или рынков.

На рисунке 3 представлена примерная схема соответствия между представлениями реального и развивающегося виртуального электронного мира.

Биометрические технологии, предлагаемые зарубежными компаниями (разработанные на основе существующих международных стандартов, базирующихся на национальных стандартах США), в силу относительной слабости, низкой надежности, слабой устойчивости к атакам подбора, обязательности присутствия проверяющего предъявляемого биометрического образа будут использоваться только в реальном мире, и не смогут быть применены в виртуальном е-мире.

Разрабатываемые новые высоконадежные биометрические средства и технологии, предлагаемые российскими производителями, исключают все указанные недостатки и способны работать в открытом информационном пространстве е-мира.

Разговор о современном уровне информатизации общества сегодня обязательно связан с термином «электронного государства/общества». Однако, построение декларируемого демократического (суть равноправного для всех) электронного государства не имеет смысла без обеспечения равнодоступных для всех граждан средств информационной безопасности. Существующий рынок средств информационной безопасности ориентирован в основном на государственные и коммерческие структуры, а средства криптографической защиты – на крупные организации. Все это ставит в неравные условия граждан, порождая электронное неравенство [2] – е-неравенство.

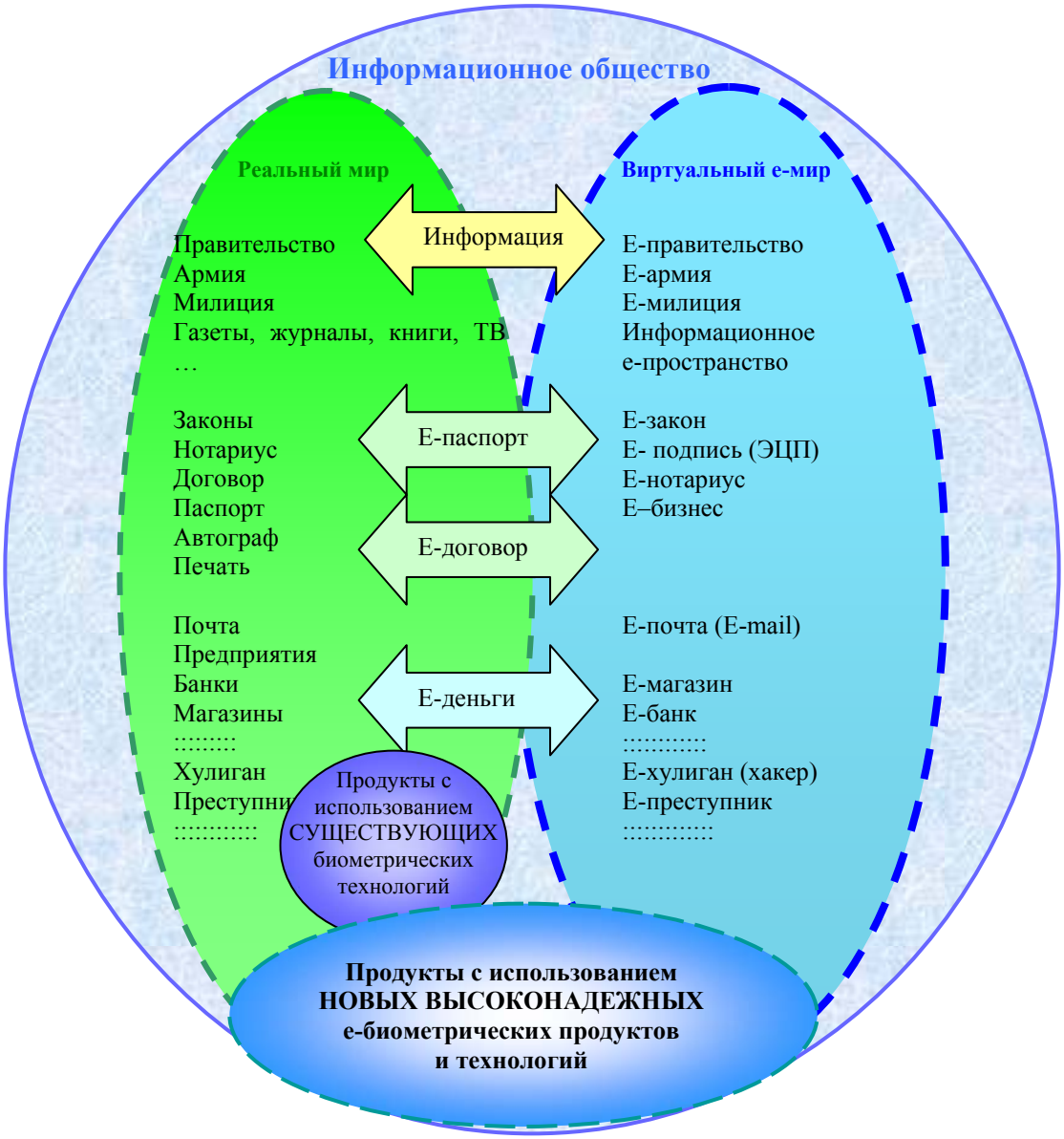


Рисунок 3 – Развитие тождественного информационного е-пространства

Для создания условий равных возможностей для всех граждан в е-государстве требуется создать рынок доступных ПЕРСОНАЛЬНЫХ электронных продуктов информационной безопасности. Требования к характеристикам этих продуктов должны быть стандартизированы [1], а сами устройства иметь сертификаты соответствия требуемым стандартам [1].

А поскольку электронное государство не имеет территориальных границ, соответственно этот рынок должен быть международным. Стратегия работы на этом рынке тоже будет международной и не зависеть от специфических условий той или иной страны. Отсюда - должна быть разработана система МЕЖДУНАРОДНЫХ стандартов, покрывающих не только реальный, но и виртуальный е-мир. Новые стандарты, очевидно, будут базироваться на основе ГОСТ-Р [1], так как в США пока нет технологий уровня предлагаемых российских, а, соответственно, нет и стандартов.

Если исходить из предположения, что к 2020 г. 10% населения будут использовать ЭЦП, и принять во внимание требования по периодичности смены ключей (не реже раза в 1,5 года) и сроке действия документа, подписанного ЭЦП (например 3-5 лет), то в конечном счете граждане, подписывающие свои документы ЭЦП, будут вынуждены хранить «связку устаревших ключей» со своими ЭЦП чтобы доказывать в суде свои права, подтверждать/опровергать ранее поставленную ЭЦП. Эту «связку» гражданин опять же должен будет прятать в некоем хранилище (сейф, банковская ячейка и т.п.), что повлечет дополнительные финансовые и организационные затраты периодически возобновляемые.

Использование биометрического хранителя информации влечет единовременную покупку с многоразовым пополнением хранимых ключей, т.е. освобождает пользователя от дополнительных затрат.

Т.о. с одной стороны, разовое финансовое вложение для рядового гражданина выгодно и привлекательно, а с другой – становление электронного государства предполагает интенсивный рост рынка недорогих высоконадежных персональных средств защиты информации и на каком-то этапе уже не будет зависеть от прироста населения, что в свою очередь привлекательно для компаний-разработчиков таких средств.

Именно поэтому Россия как разработчик первых высоконадежных биометрических средств должна занять в мире лидирующую позицию.

<u>ВЫВОД 3.</u> Перспективы роста нового сегмента рынка неограниченны в силу осознания пользователями необходимости соответствия способа обмена и защиты информации в электронном государстве и неограниченной потребности в средствах в силу непрерывного процесса регенерации физического населения.

Заключение

Заложены первые «кирпичики» в основание нового сегмента рынка средств биометрической идентификации человека.

1) Говоря о секторе на стыке рынка биометрических продуктов и технологий и рынка средств криптографической защиты информации в рамках данной статьи подразумеваются появившиеся в России (г. Пенза, ФГУП "ПНИЭИ") высоконадежные средства криптографической защиты информации, разработанные на базе биометрико-нейросетевых технологий. Данные средства могут быть применены как органами государственной власти, так и отдельными членами общества. Уникальность предлагаемых разработок заключается в отсутствии необходимости проведения организационных мер для хранения криптографических ключей с одной стороны (что является существенным при пользовании персональными средствами хранения секретной информации), а с другой – в обеспечении высокой надежности, в отличие от существующих зарубежных биометрических средств и технологий.

2) При участии специалистов ФГУП "ПНИЭИ" подготовлена окончательная редакция российского национального стандарта ГОСТ Р ТК362. Готовятся проекты еще 2 национальных стандартов.

Таким образом, сейчас Россия имеет уникальную возможность и должна приложить максимальные усилия на формирование пакета нормативно-правовых документов, регламентирующих разработку и использование НОВЫХ ВЫСОКОНАДЕЖНЫХ биометрических продуктов в России с перспективой разработки на базе национальных международных стандартов.

ЛИТЕРАТУРА:

1. ГОСТ Р 52633-2006 “Защита информации. Техника защиты информации. Требования к высоконадежным средствам биометрической аутентификации”.
2. Иванов. А.И., Анисимова Л.Ю., Акмаев А.А. Механизмы противодействия «цифровому неравенству» граждан информационного общества. // Защита информации. Inside. – 2006. - №4. - С. 2-5
3. Гезенко И.И., Иванов А.И. Обеспечение устойчивости будущего информационного общества: массовая гражданская криптография. //Защита информации. Inside. – 2005. - №1. - С. 71-79
4. Иванов А.И., Петруненков А.А. Биометрические технологии: объединение усилий и переход к этапу стандартизации. //Современные технологии безопасности. – 2004. - №3. – С. 35 – 37
5. Хруцкий В.Е., Корнеева И.В. Современный маркетинг: настольная книга по исследованию рынка: Учеб.пособие. – 2-е изд., перераб. и доп. – М.: Финансы и статистика, 2000. – 528 с.

Получено 12.06.2007 г. Опубликована в Интернет 11.09.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С 55-57. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/013)

О НЕОБХОДИМОСТИ ОРГАНИЗАЦИИ ОБЩЕСТВЕННОГО КОМИТЕТА ПО ЗАЩИТЕ ЦИФРОВЫХ ПРАВ ГРАЖДАН

Ваняшев А.В.

В России, нормативных документов, регулирующих вопросы защиты передаваемой информации, принято ограниченное количество. Так, например из международных, Федеральным законом от 19 декабря 2005 года, была ратифицирована «Конвенция о защите физических лиц при автоматизированной обработке персональных данных». Данная Конвенция была принята в Страсбурге 28 января 1981 года. Таким образом, видно, что России потребовалось 25 лет для принятия данной Конвенции у себя. Почему такое расхождение во времени? На данный вопрос можно ответить твердо – законотворчество, направленное на принятие законов о защите информации не работало.

До 2000 года в стране было принято лишь два документа, это Закон РФ от 21 июля 1993 года «О государственной тайне» и «Перечень сведений конфиденциального характера», утвержденного Указом Президента РФ от 06 марта 1997 года. Таким образом, видно, что защита информации человека как личности никого не интересовала, а интересовала защита или государственной тайны, или сведений конфиденциального характера.

Но к сентябрю 2000 года была разработана и утверждена Президентом РФ «Доктрина информационной безопасности Российской Федерации». Она представила собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Она подразумевалась стать основой для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации, подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации, разработки целевых программ обеспечения информационной безопасности Российской Федерации.

После принятия вышеуказанной Доктрины законотворчество в сфере защиты именно особо важных сведений для личности, а не для государства в целом стало набирать обороты.

Уже в январе 2002 года был принят Федеральный закон «Об электронной цифровой подписи» с целью обеспечения правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

В мае 2004 года Президента РФ издал Указ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена», который был предвестником того, что Россия ратифицирует Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных с поправками, направленных на защиту обработки данных, используемых исключительно для личных и семейных нужд, а также отнесенных к государственной тайне.

В июле 2004 года принимается Федеральный закон «О коммерческой тайне», необходимого для регулирования отношений, связанных с передачей и охраной информации, отнесенной к коммерческой тайне. Цель принятие закона была заключена в необходимости обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции.

В сентябре 2004 года была одобрена «Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года». Ее целью стало создание государственных информационных систем. В результате этого ожидается формирование эффективной системы предоставления государственных услуг на основе использования информационных технологий – «электронное правительство».

В июле 2006 года были приняты два Федеральных закона, первый – «Об информации, информационных технологиях и о защите информации», второй – «О персональных данных». Из наименования законов видно, что они направлены на внесения понятий, связанных с информацией, ее защиту, а также защиту персональных данных. Защита персональных данных личности выражается в обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Проведенный анализ развития законотворчества показал заложенные основы в сфере защиты информации, что позволит осуществлять дальнейшее принятие необходимых правовых документов.

Созданный 20 ноября 2006 года Комитет защиты цифровых гражданских прав является общественной организацией и ставит своей задачей защиту цифровых прав граждан России в Пензенском регионе. Он осуществляет свою деятельность на основе организации активного взаимодействия с исполнительными органами государственной власти области всех уровней, органами местного самоуправления, общественными объединениями, предприятиями, учреждениями и организациями различных форм собственности, обычными гражданами.

Неизбежность создания Комитета была предопределена необходимостью организовывать публичные обсуждения вопросов защиты цифровых прав граждан, которые впоследствии могут отразиться в технических решениях, технических политиках, ГОСТах, руководящих документах, административных инструкциях. Данные решения будут использоваться для поддержки цифровых гражданских прав населения в Пензенском регионе.

В состав Комитета вошли высококвалифицированные специалисты в сфере защиты информации, ставящие следующие цели:

- обсуждение вопросов защиты информации от несанкционированного доступа к персональным данным, потенциально опасных фрагментов информационных технологий и гарантии защиты от той или иной опасности;
- подготовка в установленном порядке предложений и рекомендаций техническим службам исполнительных органов государственной власти области, органов местного самоуправления Пензенской области по реализации их полномочий по вопросам поддержки цифровых гражданских прав населения в соответствии с действующим законодательством и иными нормативными правовыми актами Российской Федерации и Пензенской области;

- проведение в жизнь на территории области федеральных законов, нормативных правовых актов Президента Российской Федерации и Правительства Российской Федерации, Губернатора и Правительства Пензенской области по вопросам поддержки цифровых гражданских прав населения через соответствующие технические политики, формирование требований к поставщикам ИТ-решений;
- оценка работы муниципальных образований и государственных служащих в части реализации гражданских прав с целью выработки рекомендаций по совершенствованию этой работы с учетом изменения экономических, политических, законодательных, социальных, демографических и других условий;
- информирование граждан и общественных организаций по изменениям в законодательстве, новых технических возможностях, прогнозов на ближайшее время;
- анализ состояния правопорядка и эффективности принимаемых мер по защите цифровых гражданских прав населения;
- подготовка информационно-аналитических материалов по предупреждению правонарушений в сфере цифровых гражданских прав, внесение предложений по совершенствованию профилактической работы и устранению причин и условий, способствующих их совершению.

В заключение можно привести пример нарушения цифровых прав граждан. Всем известно, что паспорт является удостоверением личности. В случае его утери, порчи, уничтожения человеку потребуется потратить много времени на его восстановление что может повлечь нежелательные последствия. А если человек потерял паспорт (украли) во время поездки? Человек становится почти абсолютно бесправным, его личность будут устанавливать очень долго. Несчастный теряет время, возможно упускает шанс заключить договор, испытывает моральное неудовлетворение. При определенной ситуации человек может стать «рабом» гражданина, изъявшего у него паспорт (данные случаи уже «на слуху» у общественности). Необходимость срочного решения данной проблемы очевидна.

Выход есть. При повсеместном введении «электронного паспорта» все негативные последствия потери «бумажного» паспорта нивелируются. Действительно человек теряет паспорт, но его личность удостоверяется в короткий промежуток времени и он продолжает заниматься своими делами, а по приезде на свое место жительства подает заявление об утрате паспорта, и ему его выдают.

Следует заметить, что при появлении «электронного паспорта» исчезнут такие незаконные действия граждан, как кража паспорта для своих целей (жить под чужим именем, получить кредит по чужому паспорту и многие другие). Данное замечание основано на том, что личность имеет свои неповторимые физический характеристики и их подделать или украсть нельзя.

Данный пример является одним из многих, которые показывают, что введение биометрической аутентификации личности позволит решить огромное количество проблем в обществе.

Получено 12.06.2007 г. Опубликована в Интернет 11.09.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С…57-64... Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/014)

О НЕОБХОДИМОСТИ КОРРЕКТИРОВКИ ПОЛИТИКИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СВЯЗИ С ИЗМЕНЕНИЯМИ В ЗАКОНОДАТЕЛЬСТВЕ РФ В ПЕРИОД 2006-2007 г.г.

Витушкина Т. Е. ФГУП «ПНИЭИ»

XXI век характеризуется бурно развивающейся информатизацией, интенсивным внедрением средств информатизации во все сферы жизни общества. Информационная среда активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации (РФ). Национальная безопасность РФ зависит, прежде всего, от обеспечения информационной безопасности, которая является одной из ее составляющих и с развитием технического прогресса эта зависимость возрастает. В последние десятилетия XX века сохранялась устойчивая тенденция к росту убытков, связанных с компьютерной преступностью. Путем электронных ограблений в мире похищается сегодня вчетверо больше денежных средств, чем при непосредственном силовом криминальном воздействии. В странах «семерки» средний ущерб от одного компьютерного преступления достигает 450 тыс. долл. Ежегодные потери от компьютерной преступности, по оценкам экспертов, например, в Великобритании составляет 2,5 млрд. фунтов стерлингов, а в странах Западной Европы-35 млрд. долл. Эпидемия роста компьютерной преступности не обошла и Россию. По данным Совета безопасности РФ, компьютерные преступления принесли России ущерб в 1999 г. урон на сумму, равную оборонному бюджету страны [9].

С развитием конкуренции в сфере свободного предпринимательства, с ростом убытков, связанных с компьютерной преступностью, распространению которой способствует широкомасштабное применение для обработки информации средств вычислительной техники, увеличивается значимость защиты информации.

Информационная безопасность Российской Федерации – это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества, и государства [1].

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды [1]:

1. угрозы конституционным правам и свободам человека и гражданина;
2. угрозы информационному обеспечению государственной политики РФ;
3. угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
4. угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Законодательством РФ определены угрозы информационной безопасности :

1. противоправные сбор и использование информации;
2. нарушения технологии обработки информации;

3. внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
4. разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно - телекоммуникационных систем, в том числе систем защиты информации;
5. уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
6. воздействие на парольно - ключевые системы защиты автоматизированных систем обработки и передачи информации;
7. компрометация ключей и средств криптографической защиты информации;
8. утечка информации по техническим каналам;
9. уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
10. перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
11. использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
12. несанкционированный доступ к информации, находящейся в банках и базах данных;
13. нарушение законных ограничений на распространение информации.

В целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства федеральными законами устанавливается ограничение доступа к информации.

В настоящее время основные вопросы защиты информации регламентированы законами РФ «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «О связи», «Положением о государственном лицензировании в области защиты информации», а также рядом нормативно-методических документов, разработанных Федеральной службой по техническому и экспортному контролю (ФСТЭК) России.

В соответствии с ФЗ «Об информации, информационных технологиях и о защите информации», принятым Государственной думой в 2006 г.,: в области защиты информации используются следующие основные понятия

1. Информация – сведения (сообщения, данные) независимо от формы их представления [3];
2. Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [3];
3. Доступ к информации – возможность получения информации и ее использования
4. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [3].

Информационные ресурсы, являющиеся собственностью государства. находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите [4] .

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации[8]

По данным ФСТЭК России примерная структура возможных источников угроз:.

1% - случайные люди;

17% - технические средства разведки; конкурирующие фирмы, клиенты, контрагенты; криминальные структуры, террористы;

82% - собственные сотрудники организаций.

В зависимости от категории доступа, информация подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами- информацию ограниченного доступа..

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение [3].

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий [3].

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на [2]:

1. Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. Соблюдение конфиденциальности информации ограниченного доступа, реализацию права на доступ к информации;
3. реализацию права на доступ к информации.

Защита информации ограниченного доступа при ее обработке техническими средствами определяется СТР-К, государственными стандартами и нормативно-методическими документами ФСТЭК России.

На рисунке 1 отображена связь информационной безопасности с элементами общей системе безопасности предприятия.

Указом Президента РФ 1997 г. №188 определены виды конфиденциальной информации:

1. Персональные данные - сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Судебная тайна - сведения, составляющие тайну следствия и судопроизводства.

3. Служебная тайна – сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

4. Профессиональная тайна - сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами. Профессиональная тайна подлежит защите в случаях, если на лиц, владеющих такой информацией при исполнении

профессиональных обязанностей возложены обязанности по соблюдению конфиденциальности такой информации.

5. Коммерческая тайна - сведения, связанные с коммерческой деятельностью.

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

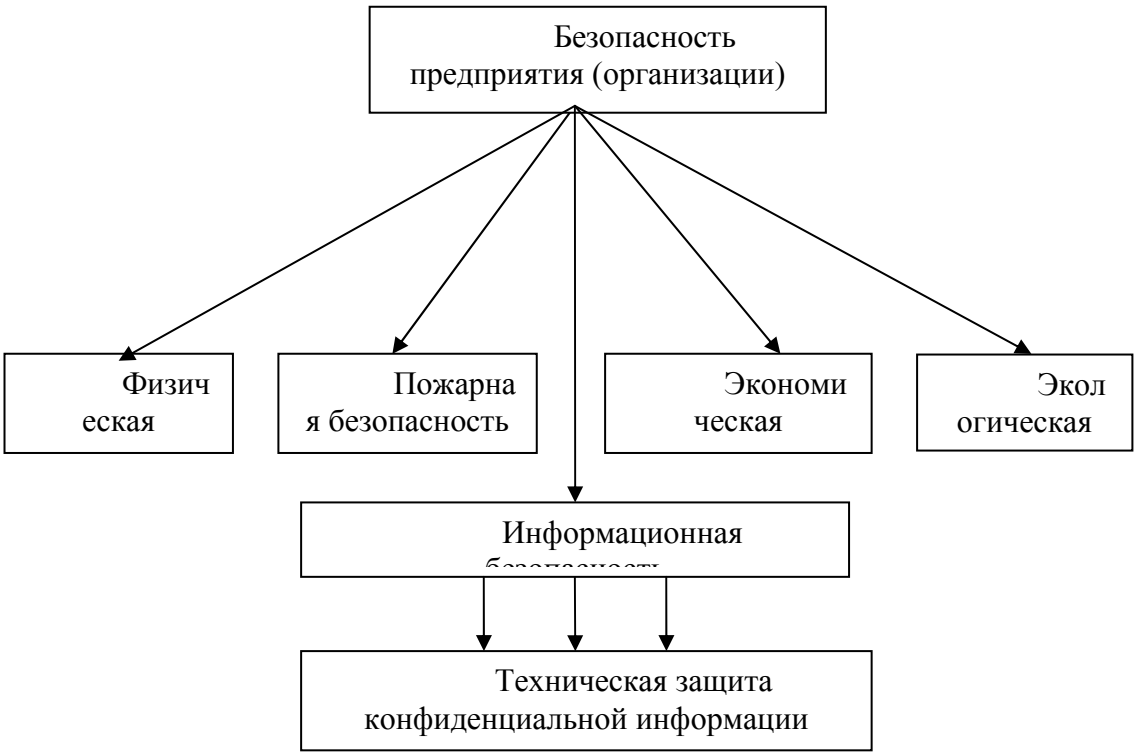


Рис. 1. Место информационной безопасности в общей системе безопасности предприятия

В первоочередном порядке подлежат защите следующие виды информации:

- речевая информация, циркулирующая в защищаемых помещениях;
- информация, обрабатываемая СВТ;
- информация, хранящаяся на физических носителях, в том числе входящих в состав автоматизированной системы (АС);
- информация, передаваемая по каналам связи, выходящим за пределы охраняемой территории.

Объектами защиты информации ограниченного доступа могут быть:

1. Средства и системы информатизации, участвующие в обработке информации - основные технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи информации ограниченного доступа, программные средства;
2. Технические средства и системы, не обрабатывающие непосредственно информацию, но размещенные в помещениях, где она обрабатывается - вспомогательные технические средства и системы (ВТСС).
3. К ВТСС относятся:

- Телефонные средства и системы;
- ПЭВМ, не участвующие непосредственно в обработке информации, но размещенные вблизи ОТСС или в защищаемом помещении;
- Системы пожарной и охранной сигнализаций;
- Системы кондиционирования;

4. Защищаемые помещения. - помещения, (служебные кабинеты, актовые залы, конференцзалы, специально предназначенные для проведения конфиденциальных мероприятий (совещаний, переговоров и т. д.) [4].

Утечка информации возможна не только с использованием технических средств, но и за счет непреднамеренного прослушивания лицами, не допущенными к ней. Такие действия возможны в результате недостаточной звукоизоляции конструкций помещений, подлежащих защите.

При обработке информации ограниченного доступа техническими средствами и циркуляции ее в защищаемом помещении возможны следующие каналы утечки:

1. Побочное электромагнитное излучение технических средств, участвующих в обработке информации;
2. Наводки информативного сигнала, обрабатываемого средствами вычислительной техники, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны;
3. Возникновение паразитной генерации в элементах технических средств;
4. Акустическое излучение речевого сигнала;
5. Электроакустические сигналы, возникающие при преобразовании акустического сигнала в электрический за счет микрофонного эффекта;
6. Виброакустический канал; (вибрация стен, перекрытий, систем отопления, вентиляции, дверей, стекловибрация).
7. Электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема информации;
8. Использование атак по сети, вирусы;
9. Прослушивание телефонных переговоров;
10. Несанкционированный доступ к информации, обрабатываемой в автоматизированной системе и несанкционированные действия с ней;
11. Хищение технических средств с хранящейся в них информацией или носителей информации;
12. Человеческий фактор.

На предприятии защита информации ограниченного доступа может быть достигнута путем проведения ряда :

1. организационно-режимных мер, которые не требуют применения специальных разработанных технических средств защиты. Они проводятся силами и средствами самих предприятий и организаций. Например:

- выбор помещения для установки технических средств и систем, участвующих непосредственно в обработке информации ограниченного доступа (ОТСС);
- выбор места для установки ОТСС в помещении;
- расположение вспомогательных технических средств (ВТСС) относительно ОТСС в помещениях;
- организация режима и контроля доступа к защищаемым объектам;
- расположение объекта относительно границ охраняемой территории

2. Применением (при необходимости) специальных технических средств защиты. Это могут быть технические средства активной защиты (сетевые фильтры, генераторы шума), средства защиты от несанкционированного доступа.
3. выявлением специальных электронных устройств перехвата информации (закладных устройств), внедренных в используемые технические средства, защищаемые помещения – осуществляется проведением специальных проверок ОТСС и ВТСС, находящихся в защищаемом помещении.

Различают пассивные и активные методы защиты информации. К пассивным методам можно отнести экранирование технических средств, применение радиопоглощающих материалов, звукоизоляцию помещений, использование источников бесперебойного питания. К активным методам защиты – применение электромагнитного зашумления объектов, сети электропитания, виброакустическая маскировка и т. д. Средства активной защиты должны быть сертифицированы по требованиям безопасности информации.

Уровень технической защиты информации ограниченного доступа, а также необходимость применения технических средств защиты определяется дифференцировано по результатам предварительного обследования защищаемого объекта с учетом соотношения затрат на проведение работ и величины ущерба, который может быть нанесен обладателю информационных ресурсов.

Федеральным законом «О персональных данных» регламентирован порядок доступа к персональным данным и их обработка с использованием средств автоматизации. Контроль и надзор за выполнением требований по защите персональных данных, на основании данного ФЗ осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности-ФСБ, а также федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации - ФСТЭК, в пределах их полномочий. На основании «Положения о государственной миграционной системе миграционного учета» от 14 февраля 2007 г. №94 определена необходимость аттестации информационных систем по требованиям безопасности информации в соответствии с нормативными правовыми актами ФСБ и ФСТЭК.

Под аттестацией объекта информатизации по требованиям безопасности информации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - аттестата соответствия подтверждается, что объект соответствует требованиям стандартов или иных нормативных документов по защите информации, утвержденных ФСТЭК России [6].

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации [6]. Только наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в «Аттестате соответствия».

В отношении сведений, подлежащих защите в соответствии нормативно-методическими документами ФСТЭК России, на предприятии должен быть оформлен перечень сведений конфиденциального характера, а также разработана разрешительная система доступа пользователей к данной информации.

Ввиду недооценки значимости защиты информации ограниченного доступа и достаточно слабой организацией защиты, в организациях, на предприятиях возникает особая опасность ее утечки и потенциальный риск нанесения существенного материального ущерба.

Статьей 17 ФЗ «Об информации, информационных технологиях и о защите информации» определена ответственность за правонарушения в сфере информации, информационных технологий и защиты информации. За разглашение или иное неправомерное использование информации ограниченного доступа, лицо, права, которого и законные интересы были нарушены, вправе обратиться в установленном порядке в суд и потребовать возмещения убытков, а также компенсации морального вреда.

ЛИТЕРАТУРА:

1. Доктрина информационной безопасности Российской Федерации, утверждена Президентом РФ 9.09.2000 г. №Пр-1895..

2 Защита информации. Халяпин Д. Б., г.Москва, 2004 г.

3 «Об информации, информационных технологиях и о защите информации», ФЗ от 27 июля 2006 г. №149-ФЗ.

4 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. №282.

5 Указ Президента Российской Федерации об Утверждении Перечня Сведений конфиденциального характера Москва, Кремль от 6 марта 1997 года № 188

6 Положение по аттестации объектов информатизации по требованиям безопасности информации, Утверждено Председателем Государственной технической комиссии при Президенте Российской Федерации Ю. Яшиным 25.11.1994 г.

7 «О персональных данных», ФЗ от 8 июля 2006 г.№152-ФЗ.

8 ГОСТ Р 50922-96 Защита информации. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ. Москва, 1996г.

9 «Государственная тайна и ее защита в Российской Федерации», Под ред. М. А. Вуса и А. В. Федорова С-Петербург Юридический центр Пресс, 2005 г.

Получено 19.09.2007 г. Опубликована в Интернет 11.10.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. с. 64-... Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/015)

АНОНИМНОСТЬ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ ВЫСОКОНАДЕЖНЫХ НЕЙРОСЕТЕВЫХ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ-КОД

Иванов А.И., Хозин Ю.В.

Биометрическую идентификацию личности по снятым отпечаткам пальцев с места преступления криминалисты используют с конца 19 века (метод предложен Г. Фулдсом и В. Гершелем в статье авторитетного английского журнала «Nature», опубликованной в 1880 году). К концу 20 века процедуру идентификации человека по рисунку линий кожи пальцев удалось автоматизировать. Сегодня – это одна из наиболее востребованных процедур биометрического контроля людей, широко используемая в паспортно-визовых документах нового поколения.

Автоматизация биометрического контроля гражданина построена на том, что в микросхеме его паспорта содержится образец отпечатка его пальца. Подменить образец эталонного отпечатка практически невозможно, так как содержание микросхемы фактически является электронным документом, хваченным электронной цифровой подписью органа МВД, выдавшего паспорт. Бланк обычного паспорта на бумажном носителе усилен электронным дополнением с криптографической защитой целостности этого дополнения.

Сама процедура биометрической проверки гражданина по его паспорту осуществляется в соответствии с блок-схемой, отображенной на рисунке 1.

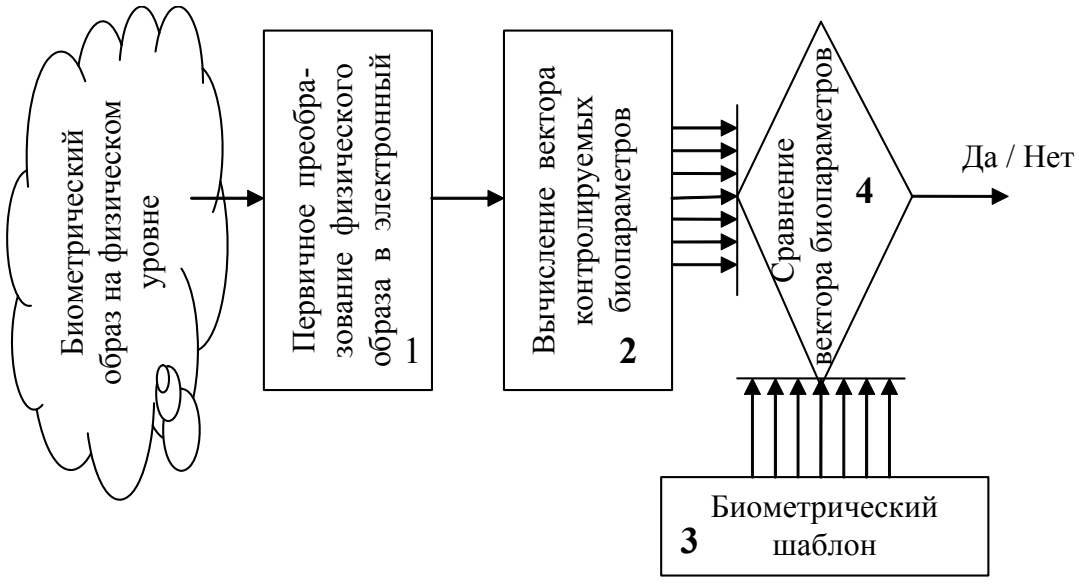


Рис. 1. Блок-схема процедур биометрической идентификации, выполненных с классическим решающим правилом

Если биометрический шаблон в паспорте и предъявленный при проверке рисунок пальца имеют много общего, то принимается автоматическое решение «Да» - это именно тот человек. По идее автоматическое решение «Да» должно открывать дверь турникета в другую страну и тем самым снять ряд проблем. Если по какой-то причине автомат даст «Нет», то офицер пропускного пункта контроля будет проводить Вашу проверку в обычном неавтоматическом режиме.

Блок-схема рисунка 1 вполне пригодна для контроля граждан, желающих въехать в страну и открыто заявляющих как свое имя, так и свое право на этот въезд. То есть для международных паспортов с автоматизированными биометрическими проверками вполне достаточно добиться понимания биометрической информации чужих иностранных паспортов национальной системой каждого из государств. Для этой цели уже создано несколько десятков международных биометрических стандартов. Нет сомнений в том, что паспортно-визовые документы нового поколения будут прекрасно работать в ближайшем будущем. Так, где требуется только контроль и не нужна поддержка анонимности гражданина международные биометрические технологии вполне и вполне применимы.

К сожалению, простой биометрический контроль человека без обеспечения анонимности его персональных данных приемлем далеко не всегда. Везде, где на ряду с контролем требуется обеспечение анонимности (голосование, электронные платежи, электронная медицина, взаимная биометрическая идентификация граждан,…) необходимо использовать специальные механизмы. Например, для сохранения анонимности проверяемого можно использовать искусственную нейронную сеть (блок-схема рисунка 2).

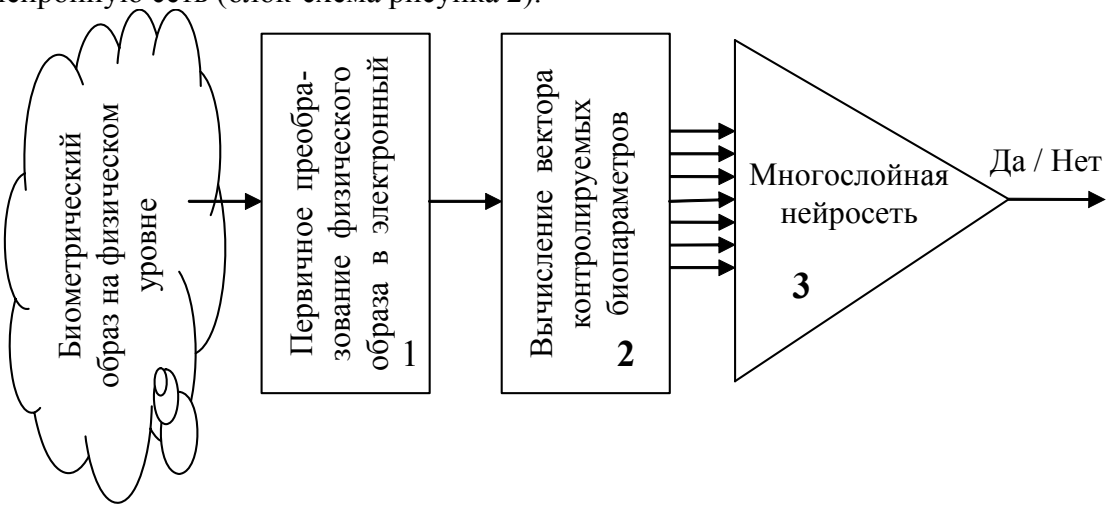


Рис. 2. Блок-схема процедур биометрической идентификации, выполненных с классическим нейросетевым решением

Если сравнивать рисунок 1 и рисунок 2, то не трудно заметить исчезновение биометрического шаблона. Во время обучения искусственной нейронной сети распознаванию человека биометрический шаблон растворяется в параметрах связей обученной нейронной сети. По таблицам связей и параметров нейронной сети нельзя узнать на какой биометрический образ она обучена. При переходе от идентификации человека по классическим правилам к нейросетевой идентификации происходит нейросетевое сокрытие конфиденциальной биометрической информации [1].

Следует отметить, что качество классических и нейросетевых решений, выполненных по блок-схемам рисунка 1 и 2 примерно одинаковое. В частности при анализе рисунка отпечатка пальца примерно в 5% случаев и то и другое технические решения будут отвергать «Своего», при этом «Своему» для положительного решения зачастую достаточно повторно предъявить свой палец (достаточно повторного сканирования рисунка). Чужой, предъявив на удачу свой палец, ошибочно получает положительное решение с вероятностью близкой к 0.001. То есть каждый тысячный самозванец сможет выдавать себя за Вас. Или каждому самозванцу до первой удачи придется примерно 1000 раз предъявлять свой палец под разными именами. Еще лучше для самозванца достать базу

авторизованных биометрических образов и заранее выявить всех людей с близкой к его биометрией (все это касается любой биометрии). Очевидно, что качества современных биометрических приложений для осуществления безопасного Интернет голосования или Интернет покупок явно недостаточно.

Для того, что бы сделать биометрию не только анонимной, но и высоконадежной национальный российский стандарт [2], требует отказаться от простых технических решений с одним выходом «Да/Нет» (от решений с низкой размерностью ключа). Для одновременного обеспечения и анонимности биометрии и высокого качества биометрического идентификационного решения предлагается применять нейросетевые преобразователи с большим числом выходов. Блок-схема процедуры высоконадежной биометрической аутентификации приведена на рисунке 3.

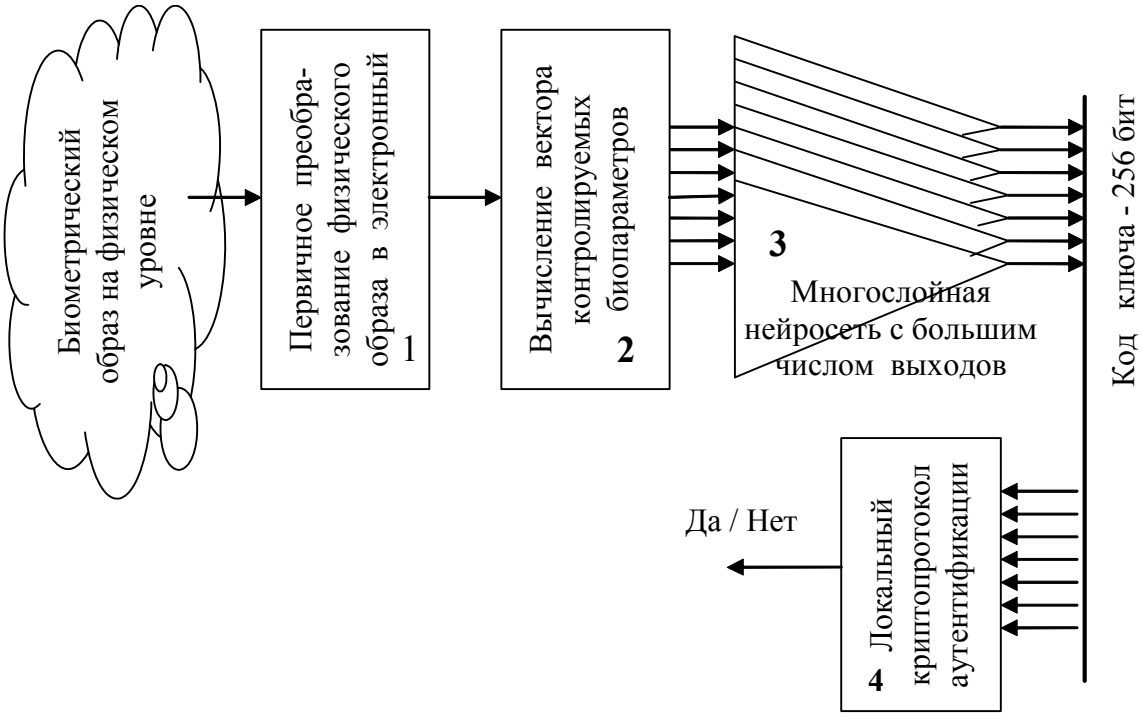


Рис.3. Блок-схема процедур биометрической аутентификации, выполненных с нейросетевым вектор-решением высокой размерности

По нашему национальному ГОСТу шифрования и ГОСТу формирования электронной цифровой подписи ключ должен иметь длину 256 бит. То есть в место одной нейросети мы должны использовать 256 нейронных сетей, причем обучить их так, что бы они давали заранее заданный ключ при предъявлении системе примеров биометрического образа «Свой». При предъявлении случайного образа «Чужой» нейросетевой преобразователь биометрия-код должен выдавать случайное число [2]. Подобная схема выполнения биометрической защиты информации позволяет одновременно и поднять качество принимаемого многомерного решения и защитить программ от атаки на «последний бит».

Традиционно считается, что программные средства защиты слабы. Усложнение решающих правила при организации программ, выполненных в соответствии с блок-схемами рисунка 1 и рисунка 2 всегда очень уязвимо. Всегда остается «последний бит» «ДА/Нет», для преодоления программной защиты достаточно найти «последний бит» и инвертировать его (либо жестко присвоить «Да всегда»). Даже если поиск «последнего бита» займет много времени, взлом окупится сторицей. После обнаружения «последнего бита» пишется программный

автомат взлома и тиражируется. В итоге программная защита через не продолжительное время перестает быть защитой.

Ситуация в корне изменяется при выполнении программной защиты в соответствии с блок схемой рисунка 3. Хакер получивший доступ к ней не может найти «последний бит», он натыкается 256 неизвестных «последних бита». Перебор всех возможных состояний ключа длиной 256 бит – это задача гарантированно высокой вычислительной сложности. Даже если при ее решении хакеру улыбнется удача тиражировать эту удачу ему не удастся. У каждого пользователя должен быть свой ключ защиты. Именно по этим причинам новая схема выполнения программ защиты гораздо надежнее традиционных и рекомендована ГОСТ Р 52633-2006 как типовая.

Все выше сказанное достаточно очевидно и проблем при осознании не вызывает. Трудности понимания возникают при осознании эффекта многократного повышения надежности нейросетевых биометрических решений высокой размерности. В связи с этим поясним именно эту ситуацию на простом примере однослойной сети всего из двух нейронов с двумя входами и двумя выходами. Эта простейшая сеть и распределения на ее входах/выходах отображены на рисунке 4.

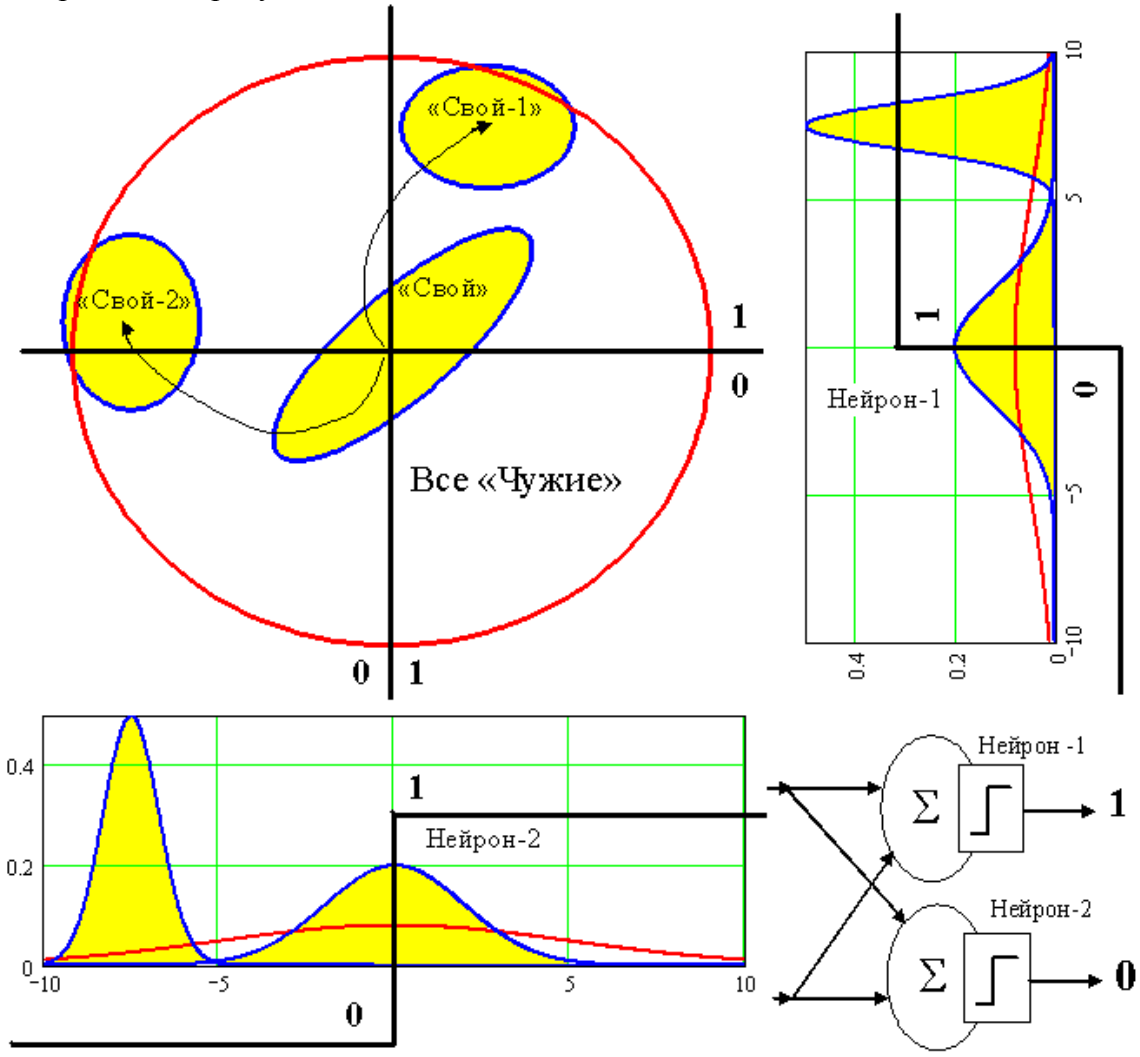


Рис. 4. Правильно обученная однослойная сеть из двух нейронов, откликающаяся кодом «10» на образ «Свой»

Как показали эксперименты биометрические образы все «Чужие» имеют близкий к нормальному закон распределения значений по любому из контролируемых биометрических параметров. Случайные образы «Чужой»

независимы и потому дают двухмерное нормально распределение, которое после нормирования по дисперсиям хорошо описывается кругом (красный цвет линий на рисунке 4). Наиболее часто биометрические параметры появляются близко к центру множества все «Чужие». В рассматриваемом нами случае первый и второй контролируемые биометрические параметры множества «Свой» сильно коррелированны и граница их распределения имеет вид эллипсоида. Обучение первого и второго нейрона однослойной сети приводит к сжатию самого множества «Свой», а так же к выталкиванию его из центра множества все «Чужие». На рисунке 4 стрелками показаны траектории движения центров множеств «Свой» при обучении первого и второго нейрона.

Для того, чтобы обучать нейросеть необходимо заранее задать выходной код, соответствующий образу «Свой», в нашем случае выходной код «Свой» соответствует комбинации «01». Для того, чтобы максимально затруднить «Чужому» случайное угадывание кода «Свой» необходимо линейные разделяющие функции строить проходящими точно через центр множества все «Чужие». В этом случае «Чужой» не знающий образа «Свой» способен угадывать каждый разряд кода с вероятностью 0,5.

Для того, чтобы нейросеть при атаках подбора работала как хэшфункция необходимо добиться независимости (некоррелированности) выходов нейронов. Для достижения этого достаточно ортогонально задавать линейные разделяющие функции выходов различных нейронов (в нашем случае разделяющие функции заданы перпендикулярными относительно друг друга). В итоге мы получили двухмерный преобразователь биометрия-код способный распознавать «Своего» с вероятностью близкой 1.0 и ошибочно пропускать «Чужого» с вероятностью 0,25 (или 2^{-2}). Столь скромные результаты сегодня никого не могут удивить, более того знатоки нейросетевого обучения легко могут показать, что описанный выше алгоритм обучения при низких размерностях задачи не является оптимальным. Для низких размерностей нейронных сетей (с малым числом входов и выходов) классические алгоритмы минимизации среднеквадратической ошибки дают гораздо лучший результат. Однако эти алгоритмы очень быстро оказываются неработоспособными при увеличении размерности решаемой задачи.

В отличии от классических алгоритмов обучения нейронных сетей новые ортогональные (декорреляционные) алгоритмы обучения [1] во первых оказываются работоспособны даже при обучении нейронных сетей с 256 входами и 256 выходами. Во вторых на базе этих алгоритмов удается полностью автоматизировать процесс обучения искусственных нейронных сетей высокой размерности. В третьих эти алгоритмы оказались очень быстрыми [1] они способны обучать большие и сверхбольшие нейронные сети за несколько секунд машинного времени. На обучение нейронных сетей таких же размеров методом обратного распространения ошибки потребуются десятки лет машинного времени. Все это в месте позволяет усилить нейросетевой интеллект биометрической защиты информации примерно в 100 раз по сравнению с низкоинтеллектуальной биометрией предыдущего поколения.

В свою очередь размеры искусственного интеллекта экспоненциально связаны с качеством принимаемых им решений. Сто кратный рост размеров искусственного интеллекта приводит к увеличению качества принимаемых им решений примерно в миллиард раз (сомневающиеся могут убедиться в этом по содержанию таблицы 2 приложения «А» нашего нового национального стандарта [2]). Еще одним способом вывода экспоненциальной связи размеров нейросетевого искусственного интеллекта с качеством принимаемых им решений может быть индукция. Выше мы показали, что двухмерная нейросеть дает вероятность ошибок второго рода на уровне 2^{-2} (или 0,25). Если продолжить

аналогичные построения и добиться ортогональности разделяющих плоскостей трех нейронов трехмерной нейросети, то вероятность ошибки снизится до величины 2^{-3} (или 0,125). Для K-мерной нейросети будем иметь:

$$P_2 \approx 2^{-K} \qquad (1),$$

происходит экспоненциальное снижение вероятности ошибок второго рода. Стойкость нейросети с 256 входами и 256 выходами к атакам подбора по этой оценке должна совпадать со стойкости криптографического ключа длинной 256 бит. Это слишком хорошо, что быть правдой.

В реальной жизни идеальной ортогональности разделяющих гиперплоскостей (полного отсутствия парной корреляции выходных разрядов нейросетевого преобразователя) добиться не удается. Стандарт [2] не требует абсолютной некоррелированности выходов нейросети (вводятся только ограничения на математическое ожидание модулей коэффициентов корреляции: $m|R| \le 0.15$). Это отражение реальных условий и реальных российских технологий обучения сегодняшнего дня. Мы можем экспериментально убедиться, в том что экспоненциальная связь размерности искусственного искусственного интеллекта и качества принимаемых им решений существует. Неидеальность практической реализации автомата обучении приводит к некоторому снижению показателя роста, то есть в место степенной зависимости (1) в реальности наблюдается связь с существенно меньшей крутизной экспоненциального снижения вероятности ошибок:

$$P_2 \approx 2^{-a\,K} \qquad (2).$$

Коэффициент ослабления a ≈ 0,15 существенно меньше единицы, его следует рассматривать как некоторый эквивалент коэффициента полезного действия нейросетевой машины обогащения биометрических данных. Если бы удалось построить идеальную машину обучения, то она была бы способна извлекать все 100% полезной информации из биометрического образа. Реально существующие сегодня машины нейросетевого обучения позволяют извлечь только 15% информации их биометрического образа и запаковать ее в нейросетевой контейнер для безопасного хранения. Для сравнения гораздо более примитивные машины обучения нейросетей по методу обратного распространения ошибки дают КПД порядка 0,3%. Новые алгоритмы обучения [1] оказались примерно 50 раз эффективнее морально устаревших. Именно это обстоятельство и позволяет постепенно переходить к применению высоконтеллектуальных средств биометрико-нейросетевой защиты информации.

Подводя итоги следует еще раз подчеркнуть, что новый национальный стандарт [2] ориентирован прежде всего на гражданское применение, то есть реализованные по его требованиям средства будут использоваться преимущественно для защиты личной информации граждан. В ближайшем будущем всем нам придется участвовать в юридически значимом электронном документообороте. То есть многим из нас придется регистрировать свои открытые ключи для оформления налоговых и таможенных деклараций, оформления электронных договоров, дистанционной аутентификации. Видимо удостоверяющие центры будут расположены в шаговой доступности и обеспечат надежную информационную поддержку сертификатов открытых ключей. Вторую часть задачи – безопасное хранение личного ключа формирования ЭЦП за самих граждан никто решать не собирается. Спасение утопающих дело рук самих утопающих. Хранить личный ключ формирования ЭЦП в КПК, ноутбуке или даже в сейфе крайне опасно. Арендовать сейф-ячейку в банке дорого и неудобно.

Единственным выходом из ситуации, видимо станут программно-аппаратные хранители личных секретов человека с высоконадежным биометрико-нейросетевым доступом к конфиденциальной информации. Если они будут

выполнены в соответствии с требованиями ГОСТ Р 52633-2006, то их стойкость к физическому взлому должна составить от 500 до 5000 часов (в место 1-:- 2 часов как у обычных сейфов) и стойкость к атакам взлома самого нейросетевого контейнера порядка 10 -:- 100 лет машинного времени при условии использования широкодоступных средств вычислительной техники. Таким показателям уже можно доверять.

ЛИТЕРАТУРА:

1. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.

2. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

Получено 12.10.2007 г. Опубликована в Интернет 11.11.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. с. 71-74. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/016)

ОЦЕНКА ИЗМЕНЧИВОСТИ ПОВЕДЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ АНАЛИЗА ИЗМЕНЧИВОСТИ ПОТРЕБЛЕНИЯ РЕСУРСОВ СЕРВИСАМИ

Лакин К.А., Шумкин С.Н.

ООО НПФ «Кристалл»

Как правило, цель, реализуемая информационными системами (ИС), состоит из множества частных целей, реализуемых субъектами, работающих в ИС. Под субъектами (в широком смысле) понимаются любые активные компоненты (персонал, процессы в вычислительной среде и проч.), выполняющие действия над объектами – пассивными компонентами. Предполагается, что доступ субъектов к объектам осуществляется через сервисы. Например, для работы с файлами используются файловые сервисы, для работы с базами данных – сервисы баз данных и т.д. Выполнение любой частной цели субъекта не возможно без наличия соответствующего набора сервисов. Используя подобный подход, представляется возможным оценить изменчивость поведения ИС в целом, анализируя изменчивость поведения (работы в ИС) субъектов путем исследования изменчивости потребления ресурсов сервисами ИС.

В качестве единого представления результатов анализа предлагается использовать такой показатель, как степень изменчивости потребления ресурсов сервисами. Изменчивость потребления ресурсов сервиса определяется активностью субъектов, использующих его для реализации своих частных целей. Очевидно, что чем выше изменчивость поведения субъекта, тем менее стабильна работа используемых им сервисов и, соответственно, выше изменчивость поведения ИС в целом. Таким образом, характеристики изменчивости потребления ресурсов сервисами являются отражением изменчивости субъектов и ИС в целом.

Изменчивость потребления ресурсов сервиса можно характеризовать объемными характеристиками потребления его ресурса по каждой из услуг с возможным разделением по субъектам или группам субъектов. Весь интервал исследования T делится на меньшие интервалы времени t, которые характеризуются парой величин p_{it} (вероятность обращения к i-сервису в интервале времени t) и v_{it} (объемная характеристика потребления ресурса i-сервиса в интервале времени t). Так для n сервисов (услуг) и m моментов времени работа может быть представлена в виде матрицы, представленной на рисунке 1. Возможна различная интерпретация работы сервисов. С одной стороны, n сервисов могут входить в состав некоторого объекта (например, сервера). В этом случае должны измеряться характеристики компонента ИС (в нашем примере – сервера) и будет оцениваться изменчивость потребления его ресурсов. С другой стороны, n сервисов могут использоваться некоторым субъектом для осуществления своих частных целей. В этом случае измеряемые характеристики будут относиться к субъекту и будут говорить о типичности или не типичности его поведения.

№ сервиса	Временные отсчеты			
	1	**2**	**…**	***m***
1	v_{11}, p_{11}	v_{12}, p_{12}	…	v_{1m}, p_{1m}
2	v_{21}, p_{21}	v_{22}, p_{22}	…	v_{1m}, p_{1m}
…	…	…	…	…
n	v_{n1}, p_{11}	v_{n2}, p_{n2}	…	v_{nm}, p_{nm}

Рисунок 1 - Представление данных о работе сервиса

Анализ изменчивости потребления ресурсов сервисами состоит из следующих этапов:

– создание эталонов изменчивости потребления ресурсов сервисами;

– сравнение текущей изменчивости потребления ресурсов сервисами с их эталонами.

Эталоны изменчивости потребления ресурсов сервисами представляют собой наборы данных, предназначенные для определения степени изменчивости их работы. Эталон создается индивидуально для каждого сервиса на временном интервале построения эталона T' (T' должно быть значительно больше T). Форма и содержимое индивидуальных эталонов приведены на рисунке 1. Создаваемый эталон – это модель нормального потребления ресурсов, характерного для сервиса в нормальной ситуации. Данная модель отражает допустимую степень изменчивости потребления ресурсов сервисами при штатной деятельности субъектов.

Эталон поведения строится следующим образом:

1) выбирается фрагмент аудита, соответствующий интервалу построения эталона T';
2) определяется интервал исследования T (например, определяется, что будет анализироваться суточная активность);
3) интервал исследования разбивается на определенное число временных отсчетов t. Например, при выборе t=10 минутам в сутках получается 144 отсчета;
4) для каждого сервиса по каждому отсчету времени t по данным аудита вычисляются значения p_{it} и v_{it};
5) вычисляются средние значения p_{it} и v_{it} для каждого сервиса на интервале построения эталона. В итоге формируется матрица, содержащая значения $p^э_{it}$ и $v^э_{it}$, размером $m \times n$, где m – число отсчетов в сутках, а n – число исследуемых сервисов (см. рисунок 1);
6) вычисляется допустимая изменчивость потребления ресурсов сервиса при штатной работе субъектов относительно его эталонного потребления ресурсов. Изменчивость потребления ресурсов может быть вычислена по формуле (1).

$$S^э_{it} = \frac{1}{p^э_{it}} \left(\frac{v^э_{it} - v_{it}}{v^э_{it}} \right)^2 . \qquad \textbf{(1)}$$

где v_{it} –объем потребленного ресурса i-го сервиса в момент времени t одного из интервалов исследования.

Для того чтобы выполнить сравнение текущей изменчивости потребления ресурсов сервиса с эталоном на предмет определения степени допустимой изменчивости, необходимо выполнить действия, аналогичные действиям при построении эталона по данным аудита за анализируемый период. В результате формируются значения v_{it}, характеризующие потребление ресурсов i-го сервиса в

интервале измерения *t*. Далее вычисляется изменчивость сервиса относительно его эталонного поведения по формуле (1).

Для того чтобы оценить насколько согласуется вычисленная изменчивость потребления ресурсов сервиса за анализируемый период времени с его эталонной (допустимой) изменчивостью, вычисленной при построении эталона, могут применяться различные методы оценки, позволяющие определить типичность (нетипичность) потребления ресурсов исследуемых элементов непосредственно по значениям параметров, вычисленным по данным аудита ИС. Например, могут применяться сигнатурные и/или статистические методы [1].

Таким образом, применение подобного подхода к оценке поведения ИС в целом на основе анализа изменчивости поведения (работы в ИС) субъектов путем исследования изменчивости потребления ресурсов сервисами ИС дает следующие преимущества по сравнению с другими подходами:

- в формировании изменчивости принимают участие не только значения снимаемых параметров, но и вероятности их использования, что значительно повышает качество оценки;
- данный подход позволяет оценивать в одном базисе разные параметры.

ЛИТЕРАТУРА:

1 Лакин К.А. Статистические методы анализа данных аудита в системах обнаружения вторжений. Труды научно-технической конференции «Безопасность информационных технологий». Том 3. С.7-10.

Получено 15.10.2007 г. Опубликована в Интернет 11.11.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. с. 75-... Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/017)

ТРЁХПОЗИЦИОННЫЙ СЕЙСМИЧЕСКИЙ КОМПЛЕКС ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ГРУПП

Захаров С.М.

Институт систем управления и информационной безопасности Пензенского государственного университета.

Данная статья посвящена возможности создания мобильного трёхпозиционного комплекса, работающего на сейсмическом принципе обнаружения. Основная задача, решаемая мобильным трехпозиционным комплексом, является обеспечение безопасности мобильных групп. Комплекс позволяет обнаружить пешего нарушителя (или группу нарушителей), вторгшихся на контролируемый участок местности, а так же определить зону, в которой находится нарушитель.

В основе системы лежит сейсмический обнаружитель человека и группы людей, использующий пространство признаков высокой размерности. Теоретическую основу такого подхода составляет «теорема Ковера о разделимости образов», которая утверждает следующее: «Нелинейное преобразование сложной задачи классификации образов в пространство более высокой размерности повышает вероятность линейной разделимости образов». В качестве такого нелинейного преобразования используется корреляционный функционал.

Для начала рассмотрим фрагмент типового сейсмического сигнала человека, идущего на расстоянии 50 м от сейсмического приемника (СП), и огибающая этого сигнала показаны на рисунке 1.

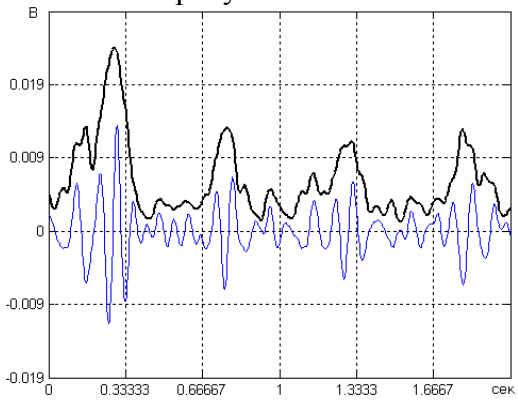


Рисунок 1- Сейсмический сигнал идущего человека и огибающая сигнала

Огибающая полезного сигнала в дальнейшем используется как информативная составляющая. Она может быть выделена любым известным методом на стадии предварительной обработки сигналов.

Для формирования признакового пространства используется корреляционный функционал, рассчитываемый по следующей формуле:

$$M1_{i,j} = \frac{\sum_{k=0}^{N}\left(x_{i+k} - \frac{1}{N}\sum_{k=0}^{N}x_{i+k}\right)\cdot\left(x_{i+j+k} - \frac{1}{N}\sum_{k=0}^{N}x_{i+j+k}\right)}{\sqrt{\left(\sum_{k=0}^{N}\left(x_{i+k} - \frac{1}{N}\sum_{k=0}^{N}x_{i+k}\right)^2\right)\cdot\left(\sum_{k=0}^{N}\left(x_{i+j+k} - \frac{1}{N}\sum_{k=0}^{N}x_{i+j+k}\right)^2\right)}},$$

где x – вектор дискретных отсчетов значений огибающей сигнала; N – длительность временного окна в отсчётах, j – номер признака. В текущей версии алгоритма N=60, j=1..200, т.е. используется двухсотмерное признаковое пространство.

Для уверенного обнаружения движущегося объекта и уменьшения числа ложных срабатываний время анализа исходного сигнала для принятия решения должно составлять несколько секунд. Чем больше отношение сигнал/шум, тем меньше времени требуется для принятия решения. В рассматриваемом алгоритме время анализа сигнала составляет 6 с при периоде принятия решения об обнаружении, равном 1 с.

Усреднение матрицы признаков $M1$, за 6 с анализа с использованием зависимости

$$M2_{i,j} = \frac{1}{6}\sum_{k=0}^{5} M1_{i+k,j},\ i = 0, 1, 2, \ldots$$

позволяет существенно уменьшить влияние случайных факторов.

В матрице $M2$ содержится информация о среднем периоде шагов. Для обработки признакового пространства используется набор линейных преобразователей, представленный в виде матрицы $M3$, ее коэффициенты вычисляются по сигналам с заранее известным средним периодом шагов. Матрица $M3$ показана на рисунке 2.

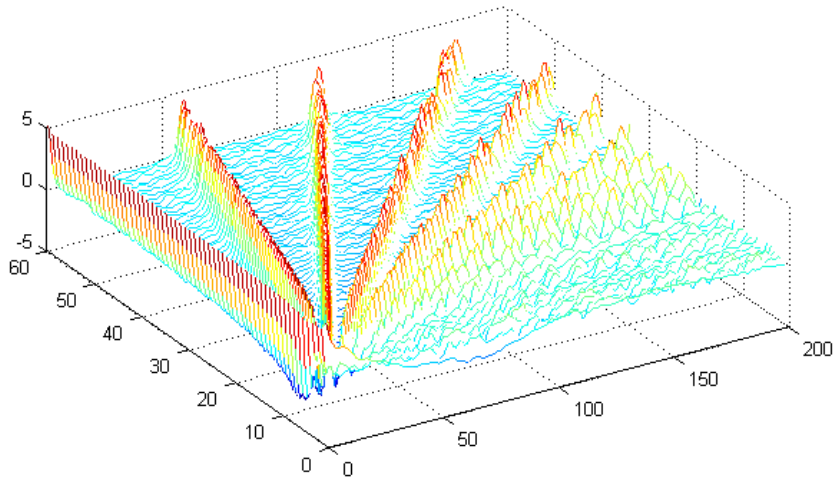


Рисунок 2 – коэффициенты линейных преобразователей.

Преобразование можно представить как $M2 \times M3$. В рассматриваемом алгоритме было использовано 60 линейных преобразователей.

Далее необходимо найти максимальное значение произведения матриц, т.е. номер линейного преобразователя максимально близкого к анализируемому примеру. Как уже сказано выше, коэффициенты линейных преобразователей

вычисляются по примерам с заранее известным периодом, либо по примерам помех. Таким образом, по индексу линейного преобразователя получившего максимальное значение можно вычислить среднегрупповой период шагов одного человека или группы людей либо отнести к какому либо классу помех, а само максимальное значение произведения использовать в качестве параметра, характеризующего наличие/отсутствие объекта в зоне обнаружения.

На рисунке 3 показан результат работы алгоритма по рассматриваемому в качестве примера сигналу. На рисунке 3а приведен исходный сигнал и сигнал обнаружения, на рисунке 3б показан график изменения рассчитанного среднего значения периода шагов, на рисунке 3в – порог принятия решения и график изменения максимального значения произведения матриц.

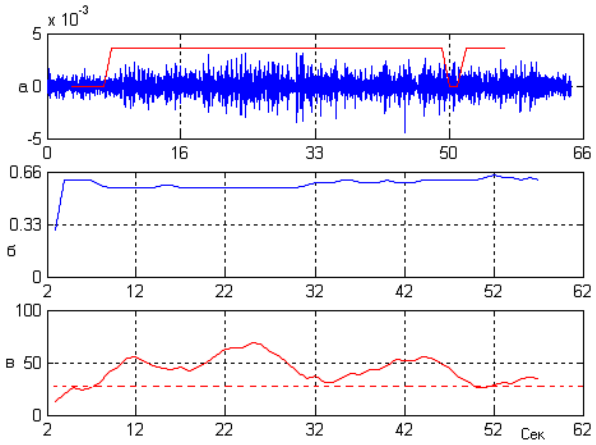


Рисунок 3- Результат тестирования алгоритма обнаружения по сигналу идущего человека

Показательным свойством любого алгоритма обнаружения является помехоустойчивость его работы. Для оценки помехоустойчивости рассматриваемого алгоритма были произведены записи сигналов сейсмического фона в условиях леса при порывах ветра до 18 м/с. Результат показывает воздействия большой сейсмической помехи, обусловленной движением корней деревьев, алгоритм дает ложного срабатывания.

При тестировании алгоритма на реальных сигналах, записанных в полевых условиях, получено значение вероятности обнаружения движущегося человека или группы людей не ниже 0.98 в радиусе до 70 м. Вероятность ложных срабатываний при тестировании на сигналах разного вида естественных помех не превысила 0.001. В условиях леса дальность обнаружения человека или группы людей уменьшается до 30 м. Задача обнаружения решается для объектов передвигающихся шагом, бегом, на лыжах, по-пластунски. Представленный алгоритм хорошо работает на любом типе грунта, и, как правило, не требует индивидуальной настройки для него.

Использование данного алгоритма даёт возможность создать на его базе быстро разворачиваемый комплекс, состоящий из трёх сейсмических обнаружителей, связанных по радиоканалу с носимым приёмником.

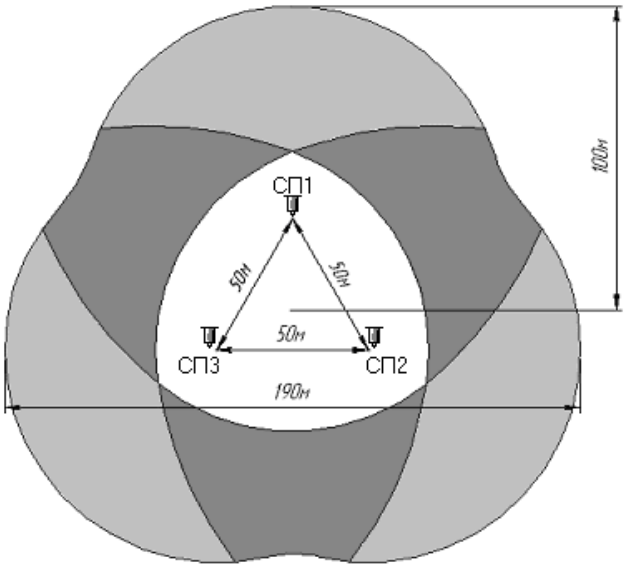


Рисунок 4- Схема расположения и зоны обнаружения
мобильного комплекса

Сейсмоприёмники располагаются в вершинах равностороннего треугольника. При таком расположении удаётся получить семь независимых зоны обнаружения, общая протяжённость охраняемого периметра 1300м. Особенностью данного комплекса является то, что мобильная группа может находиться в центральной зоне обнаружения, не влияя на возможность обнаружения нарушителя на подходах к периметру. При необходимости центральная зона может быть разбита ещё на несколько зон. В реальном времени система выдаёт номер зоны, в которой находится нарушитель. В случае обнаружения нарушителя одним из датчиков на носимый приёмник передаются максимальные значения произведения матриц $M2 \times M3$ (2 байта). Номер зоны определяется путём сравнения максимальных значений произведения матриц полученных с каждого обнаружителя.

Использование трёх датчиков позволяет получить следующие преимущества перед аналогичными комплексами:

1) быстрая установка на местности;
2) малая масса и габариты при переноске;
3) малое энергопотребление;
4) пониженные требования к радиоканалу;
5) низкая стоимость.

Исходя из этих преимуществ, такой комплекс является перспективным и востребованным. Приведенный выше пример является хорошей иллюстрацией того, что повышение размерности задачи и действительно многомерная обработка позволяют извлекать существенно большее информации и не только обнаруживать присутствие «Чужого» нарушителя, но и определять зону его присутствия. Активные «Свои» находящиеся в центральной зоне не влияют на способность системы обнаруживать вторжения.

Получено 20.10.2007 г. Опубликована в Интернет 11.11.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С…79-81. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/018)

ИЗВЛЕЧЕНИЕ ПСЕВДОДИНАМИКИ ИЗ «МЕРТВОЙ» РУКОПИСНОЙ НАДПИСИ ПРИ АВТОМАТИЗИРОВАННОМ АНАЛИЗЕ ДОКУМЕНТОВ НА БУМАЖНОМ НОСИТЕЛЕ

Воячек С.А.

Пензенский государственный университет

Известно, что высоконадежные нейросетевые преобразователи биометрия-код [1] построены на использовании динамики воспроизведения «живой» рукописной парольной фразы. Колебания пера X(t), Y(t) при воспроизведении рукописного слова нормируются и раскладываются в ряд Фурье, косинустные и синусные коэффициенты которого далее используются для нейросетевой обработки. Биометрические данные, полученный при воспроизведении «живой» рукописной надписи удобны тем, что они оказываются упорядочены во времени.

В связи с тем, что нейросетевые преобразователи биометрия-код могут иметь большие и сверхбольшие размеры по числу анализируемых параметров, числу нейронов, числу слоев нейронов, числу связей, числу выходов они на данный момент обладают рекордно высоким качеством принятия нейросетевого решения. По факту нейросетевые анализаторы статических «мертвых» рукописных образов оказываются существенно слабее нейросетевых анализаторов динамики «живых» рукописных образов. В связи этим возникает задача извлечения псевдодинамики из отсканированных «мертвых» рукописных образов. Пример такого образа приведен на рисунке 1.

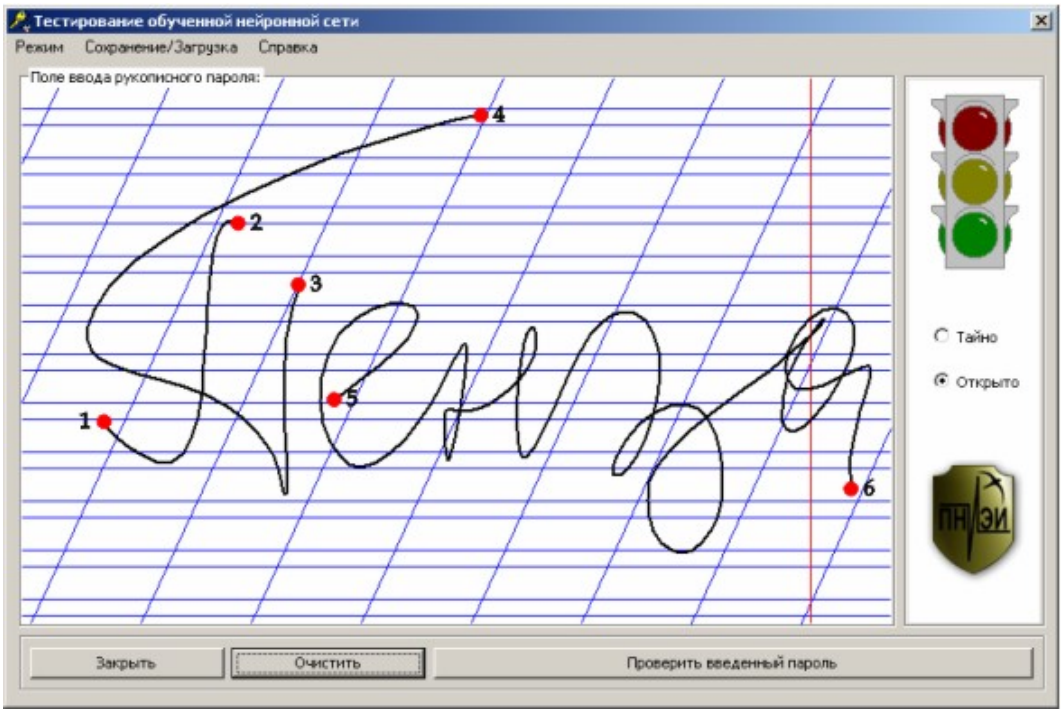


Рис. 1. Пример рукописной надписи «Пенза» с 6 отрывами пера, отмеченными нумерованными точками

Первоначально исходное растровое изображение необходимо очистить от шума, удалить фон и очертить контуры изображенных кривых. В случае рукописной надписи известно, что надпись состоит из набора отдельных кривых, каждая кривая ограничивается точками отрыва пера. Поэтому целесообразно следующим шагом определить координаты таких точек, как показано на рисунке 1.

Далее необходимо выделить отдельные кривые движения пера и получить их псевдодинамическую характеристику. В качестве исходной выбираем точку отрыва, имеющую минимальное значение абсциссы. Условно предполагаем, что перо берет начало своего движения именного из данной вершины. Скорость движения пера опередим равной некоторой постоянной величине. Движение по выбранной траектории осуществляем по тех пор, пока не будет достигнута очередная точка отрыва. В случаях, когда одна траектория пересекает другую, направление дальнейшего движения выбирается согласно правила инерции, т.е. вторые производных функций X(t) и Y(t) должны быть близки 0, т.к. предполагается, что перо движется плавно.

Блок схема программы, реализующий предлагаемый алгоритм представлена на рисунке 2.

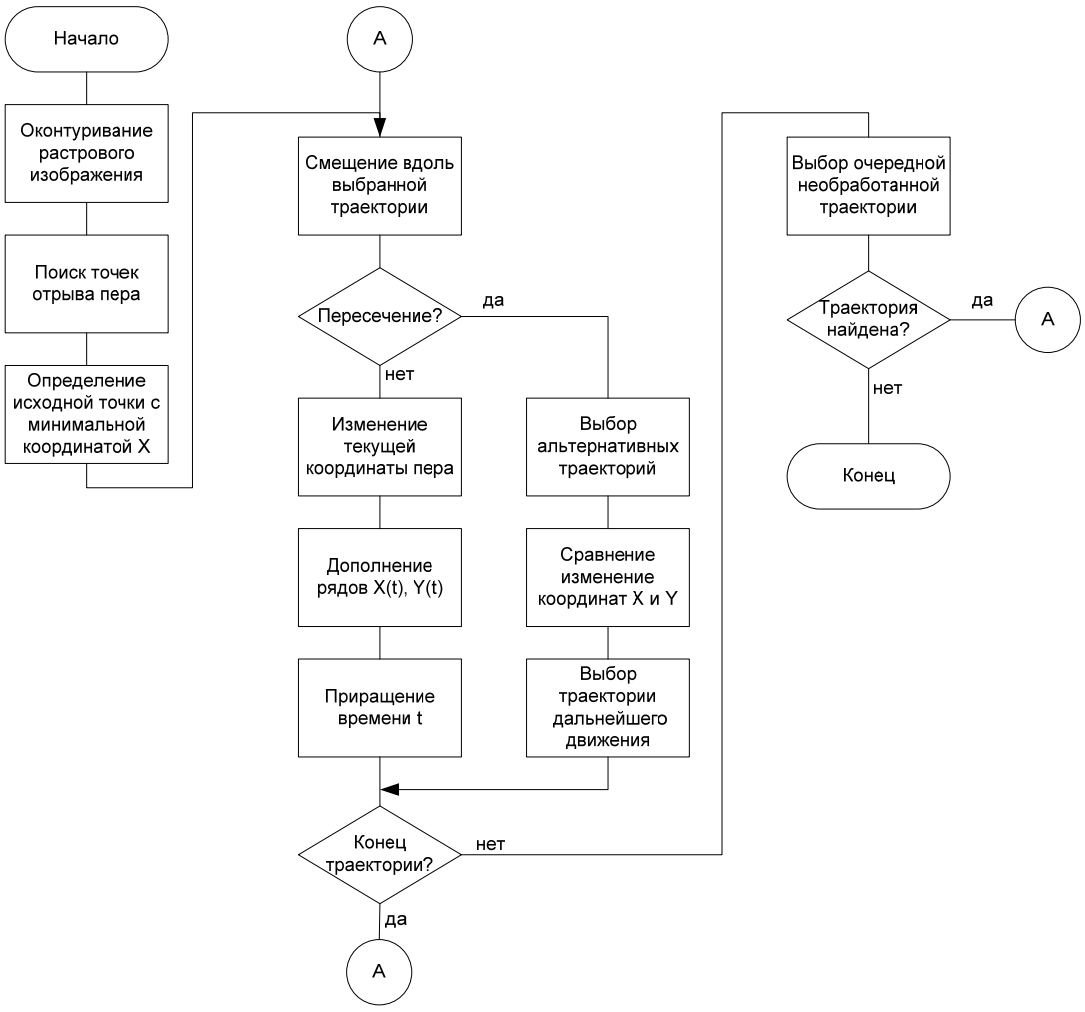


Рис. 2 Блок-схема программы извлечения псевдодинамики

После обработки отдельной траектории переход к следующей траектории осуществляется по принципу максимальной близости точки отрыва текущей

траектории и точки отрыва следующей. Важно, что точки и траектории, обработанные ранее, не участвуют в дальнейшей обработке. Так, например, на рисунке 1 точки отрыва пронумерованы в порядке последовательности их обработки.

Стоит отметить, что представленный алгоритм имеет ряд неопределенностей. Первая из них, это неопределенность выбора начальной и конечной точки кривой. Растровое изображение не дает представления о том, откуда перо начало свое движение. Следующей неопределенностью является выбор очередной точки отрыва, т.к. не гарантируется, что перо будет помещено в точку, ближайшую к текущей.

Оба рода неопределенностей имеет конечное число альтернатив, поэтому могут быть разрешены. Предлагаемый алгоритм может быть дополнен получением не только наиболее вероятного варианта псевдодинамики, но и других, менее вероятных вариантов этой характеристики. Имея в своем распоряжении несколько вариантов псевдодинамики, возможна оценка близости каждого из них эталонной.

Рассмотренный в данной статье алгоритм предварительной обработки биометрических данных позволяет извлекать пседодинамическую характеристику рукописных надписей из «мертвого», растрового источника, на достаточном для применения в системах биометрической защиты уровне.

Литература:

1. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г. Издательство Пензенского государственного университета, 273 с.

Получено 20.11.2007 г. Опубликована в Интернет 1.12.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С. 82-83. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/019)

МОДЕЛЬ ПОТЕРИ ВИДИМОСТИ В КОРПОРАТИВНОЙ ЗАЩИЩЁННОЙ СИСТЕМЕ ОБМЕНА ДАННЫМИ

Колотков А.Ю., Лупанов М.Ю.
Пензенский государственный университет

Под термином «корпоративная защищённая система обмена данными» подразумевается система обмена данными (СОД) на базе специализированной аппаратуры передачи данных (АПД).

Исследование характеристик существующих защищённых СОД сложной конфигурации при воздействии различных факторов в настоящее время представляет большой интерес. Однако проведение подобных исследований на реальных объектах затруднено, а зачастую невозможно, в частности, по следующим причинам:

а) натурные эксперименты по исследованию сети могут проводиться только на её уже развёрнутых конфигурациях, для исследования каких-либо других конфигураций сетей на базе специализированной АПД потребовалось бы переконфигурировать уже развёрнутые сети;
б) при исследовании системы особый интерес представляют режимы её работы в условиях активного воздействия на систему злоумышленника, что возможно лишь при его непосредственном присутствии;
в) АПД, входящая в состав УКВ радиосети с множественным доступом, может размещаться как на стационарных объектах, так и на подвижных, в последнем случае с точки зрения исследования СОД интересна ситуация, когда подвижные объекты могут кратковременно заезжать за естественные преграды и соответственно выходить из зоны радиовидимости друг друга, что на практике возможно лишь в условиях определённого рельефа местности.

Замещение при исследовании реальных объектов их моделями позволяет преодолеть эти, а также многие другие трудности.

Причём подходы к построению моделей, позволяющих исследовать систему в различных конфигурациях и при активном воздействии на неё противника, описаны во многих работах и широко применяются во многом благодаря наличию подобных же трудностей при исследовании различных систем и объектов в других предметных областях [2].

Ситуация же потери подвижными объектами системы радиовидимости друг друга является достаточно специфичной и подход к построению модели, позволяющей исследовать её, ещё не сформирован. Однако, как показывает практика, данная ситуация оказывает довольно большое влияние на характеристики защищённых СОД, оставаясь при этом одним из наименее изученных факторов, непосредственно влияющих на работу системы.

Предлагаемая модель потери видимости между подвижными объектами, на которых расположены комплекты специализированной АПД, входящие в состав СОД, при движении по пересеченной местности представляется в виде *модели отказов и восстановлений*. Как было отмечено выше, подвижные объекты могут в процессе движения выходить из зоны радиовидимости друг друга, а затем опять входить. При этом канал связи между ними то пропадает, то восстанавливается, что иллюстрируется на рисунке 2.

Данная модель характеризуется распределением времени работы T_P и отказов T_O. В качестве параметров модели удобно использовать среднее время работы до отказа $\overline{T}_P$ и среднее время восстановления $\overline{T}_O$.

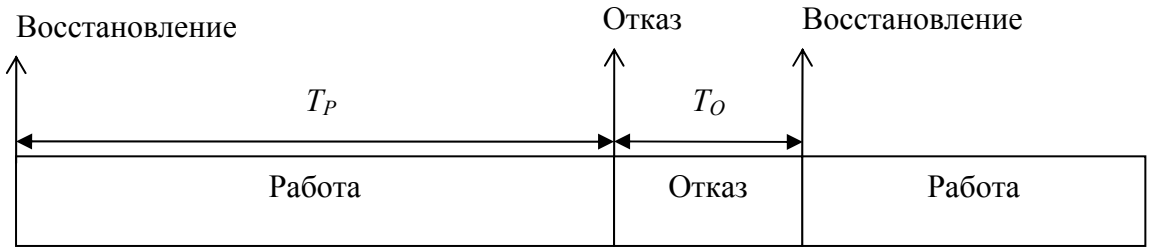


Рисунок 2 – Модель отказов и восстановлений

Однако, при моделировании защищённых СОД, как правило, среди основных подсистем выделяют непосредственно комплекты АПД и каналы, а модели этих подсистем относятся к классу моделей систем массового обслуживания (СМО)[3] и характер процессов, протекающих в этих системах, позволяет отнести их к классу дискретных систем, так как изменения состояний (например, состояний занят/свободен) происходят скачкообразно и в строго определенные моменты времени, что обусловлено тактированием аппаратуры. Так как таких систем множество, и выходы одних являются входами других, то в конечном итоге образуется сеть массового обслуживания, состоящая из СМО в дискретном времени.

Тогда при переходе к дискретной модели параметры $\overline{T}_P$ и $\overline{T}_O$ преобразуются к вероятности отказа p_o на интервале дискретного времени $T_{ДВ}$ и вероятности восстановления $p_в$ на интервале дискретного времени $T_{ДВ}$. Эти вероятности можно выразить через среднее время работы до отказа и среднее время восстановления следующим образом:

$$p_o = T_{ДВ} / \overline{T}_P,\ p_в = T_{ДВ} / \overline{T}_O \quad при \quad T_{ДВ} << T_P \quad и \quad T_{ДВ} << T_O .$$

В качестве интервала дискретного времени удобно использовать время передачи одного бита в канале.

Предлагаемая модель потери видимости между подвижными объектами может быть интегрирована в общую модель защищённых СОД, как аналитическую, так и имитационную или комбинированную.

Так, например, при имитационном моделировании время отказа в интервалах дискретного времени будет выражаться как

$$n_o = \ln(1-P) / \ln(1-p_в),$$

а время работы как

$$n_p = \ln(1-P) / \ln(1-p_o),$$

где P – случайная величина, равномерно распределенная на интервале [0,1).

ЛИТЕРАТУРА:

2 Моделирование вычислительных систем/ И.Н.Альянах. - Л.: Машиностроение, 1988. – 223 с.

3 Клейнрок Л. Теория массового обслуживания. Пер. с англ./– М.: Машиностроение, 1979. – 432 с.

Получено 22.11.2007 г. Опубликована в Интернет 1.12.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С 84-86... Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/020)

ФОРМИРОВАНИЕ БАЗ БИОМЕТРИЧЕСКИХ ОБРАЗОВ ЛЮДЕЙ, НАХОДЯЩИХСЯ В ПОЛЕВЫХ УСЛОВИЯХ, ДЛЯ ТЕСТИРОВАНИЯ СРЕДСТВ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Ю.И. Олейник
Пензенский артиллерийский инженерный институт

Использование нейросетевого преобразования биометрических данных человека в стойкий код доступа к информационным ресурсам, к особо важным объектам требует особого подхода к вопросу тестирования средств высоконадежной биометрии. При этом оценка условий, в которых находится носитель биометрического образа и его психофизиологическое состояние играют немалую роль в процессе тестирования. Необходимо учитывать это как в процессе обучения нейросетевого преобразователя биометрия-код, так и в процессе его тестирования. С целью тестирования данных устройств необходимо собирать базы данных реальных биометрических образов по специальным методикам [1].

Одно из главных требований [2], является наличие средств встроенного контроля вероятности ошибок средств защиты или вероятности удачи атаки подбора. Рукописный (голосовой) пароль может оказаться слабым и не обеспечит необходимую (декларированную производителем) стойкость защиты к атакам подбора. Чтобы убедиться в стойкости нейросетевой защиты на конкретном биометрическом образе после обучения нейросети необходимо протестировать стойкость преобразователя с использованием специально созданных баз биометрических образов.

Для решения перечисленных выше вопросов был проведен натурный эксперимент. Его целью явлось формирование и изучение натуральных баз биометрических образов (написания слова-пароля) в реальных условиях при воздействии физических нагрузок (выполнении силовых упражнений и преодоления полосы препятствий). Эксперимент включал в себя три этапа работы: подготовительный этап, подготовка личного состава, привлекаемых к тестированию, и проведение эксперимента.

В ходе выполнения подготовительного этапа производится подготовка аппаратуры и настройка программного обеспечения. В качестве аппаратуры выступает ноутбук с электронным планшетом «Genius Wizard Pen 5x4». В качестве программного обеспечения используется программа «Нейрокриптон» (ФГУП ПНИЭИ). В ходе подготовительного этапа производится подготовка инструктора, который в ходе эксперимента должен будет управлять процессом сбора биометрических образов тестируемых, формирование словаря слов-паролей, изучение места проведения эксперимента и оборудование рабочих мест для снятия биометрических характеристик. В качестве словаря использован русский орфографический словарь Российской академии наук под редакцией В.В. Лопатина, содержащий 162241 слов [1]. Для выбора слов был создан программный модуль, осуществляющий случайную выборку по данному словарю, исходя из индекса включенных в него слов. Пример полученной выборки:

43123 избранничество
5312 бабр

123541 ретинит
76512 нетарифный
34766 жаккард
452 автогамия

Накануне проведения эксперимента, на основании данных группы психологического отбора, проводится отбор испытуемых, имеющих наиболее высокий коэффициент стабильности психофизиологического состояния. С целью неразглашения личных биометрических данных испытуемых проводится кодирование их списка.

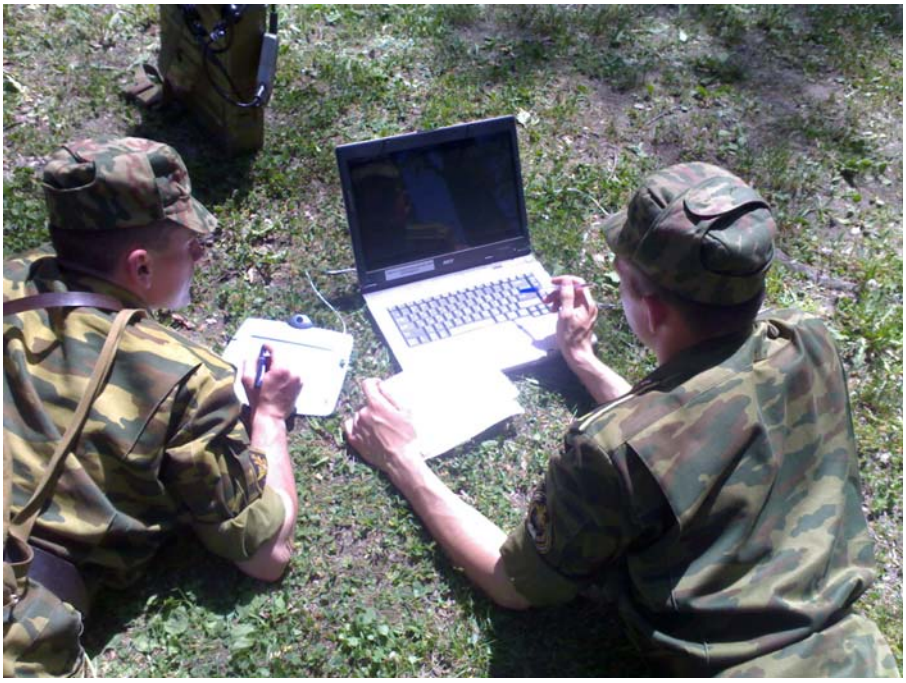


Рисунок 1. – Рабочий момент формирования базы биометрических образов в особых условиях

В ходе выполнения второго этапа, который проводится накануне эксперимента, проходит разъяснение курсантам целей эксперимента, порядка, времени, места проведения, доводятся меры безопасности. На этом этапе проводится обучение курсантов пользованию программой «Нейрокриптон», графическим планшетом и пером. Убедившись в получении стабильных навыком в работе с программой, курсанту предлагается написать 20 образов слова-пароля с запоминанием в базу данных под присвоенным номером, с обязательным контролем правильности написания слов инструктором и хронометражем времени написания. Далее проводится обучение нейросетевого преобразователя на собранных образах с протоколированием класса стойкости, выданной программой «Нейрокриптон».

После выполнения процедуры обучения нейросетевого преобразователя биометрия-код, проводится проверка системы на «пропуск своего» (ошибка первого рода), регистрация времени и количества попыток до получения курсантом физической нагрузки и после неё (курсант в упоре лежа делает 30 отжиманий).

Третий этап эксперимента проводится на полосе препятствий. Загрузив базу образов слова-пароля, собранных накануне данным курсантом, в программу «Нейрокриптон» проводится обучение нейросети, при этом слово-пароль не напоминается. Курсант воспроизводит слово-пароль на планшете. При этом

регистрируется время и количество попыток. Далее курсант выполняет упражнение на полосе препятствий.

Сразу после финиша курсант повторяет операцию по входу в систему путем написания слова-пароля. Идет регистрация времени и числа попыток. Для оценки влияния физической нагрузки на стабильность написания слова-пароля курсант вводит 20 образов предложенного слова-пароля с запоминанием в базу данных под присвоенным номером (под обязательным контролем правильности написания слова-пароля инструктором и хронометражем времени написания). Далее проходит обучение нейросетевого преобразователя на собранных образах с протоколированием класса стойкости.

Собранные в реальных условиях базы биометрических образов написания слова-пароля позволяют использовать их при обучении нейросетевого преобразователя биометрия-код и комплексного тестирования средств высоконадежной биометрии с учетом психофизиологического состояния пользователей данных систем в особых условиях. При этом на этапе обучения и определения стойкости системы к атакам подбора биометрического пароля планируемый пользователь должен повторить весь цикл описанной выше методики.

Литература

1. *Волчихин В.И.* Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации/ *В.И. Волчихин, А.И. Иванов, В.А. Фунтиков.* - Пенза: Изд-во Пенз. гос. ун-та, 2005, - 273 с.
2. ГОСТ Р 52633 - 2006 «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации».
3. *Малыгин А.Ю.* Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации /*А.Ю. Малыгин, В.И. Волчихин, А.И. Иванов, В.А. Фунтиков.* - Пенза: Изд-во Пенз. гос. ун-та, 2006, - 161 с

Получено 22.11.2007 г. Опубликована в Интернет 1.12.2007.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 7. С 87-89. Секция-2: Информационная безопасность сложных систем.
Пенза-2007 (http://beda.stup.ac.ru/RV-conf/v07/021)

ОПТИМИЗАЦИЯ ДРУЖЕСТВЕННОГО ИНТЕРФЕЙСА ФОРМИРОВАНИЯ СТАТИСТИК РУКОПИСНОГО ВОСПРОИЗВЕДЕНИЯ БУКВ ПОЛЬЗОВАТЕЛЕМ

Елфимов А.В. ФГУП «ПНИЭИ» НИП «АРГУС»

При проектировании средств биометрической идентификации неизбежно встает вопрос обеспечения дружественного интерфейса, от которого напрямую зависит желание пользователей использовать программный продукт.

Проблема ввода информации в программу определения биометрических статистик рукописного ввода заключается в том, что для ее работы требуется ввод пользователем большого количества рукописных данных, которые должны обеспечивать эквивалентное отражение многомерных статистических данных по всему множеству комбинаций символов вводимых пользователем.

Интерфейс формирования статистик должен предоставлять инструменты для взаимодействия программы с пользователем, получения и накопления необходимой информации о личных статистиках рукописного ввода. Помимо этого он должен экономить ресурсы пользователя и являться компромиссом между дружественностью и полнотой сбора данных.

Ключевым элементом интерфейса программы анализа рукописного ввода представляет собой поле ввода (Рис.1), в которое вводятся с помощью устройства рукописного ввода буквы, используемые в непосредственной работе приложения для формирования статистик.

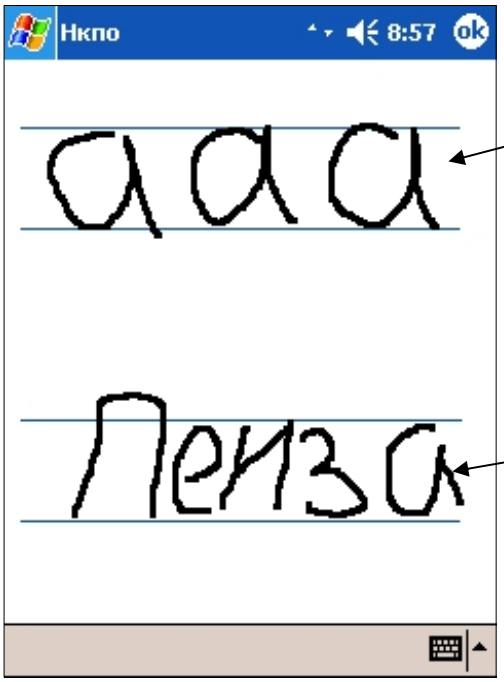


Рисунок 1. Поле ввода

Для формирования статистических данных ввода необходимо запрашивать у пользователя образцы написания всех символов используемого алфавита. Однако для удовлетворительного распознавания символа одного ввода обычно не хватает, и эффективность работы напрямую зависит от количества данных предоставленных пользователем. Для уверенной идентификации символа

приложением пользователю необходимо произвести не менее трех рукописных вводов данного символа для формирования статистических данных.

Написание рукописных символов изменяется в широких пределах даже в рамках одиночной буквы. Возможна ситуация, когда почерк человека обладает высокой нестабильностью и при трех вводах еще не удается собрать необходимые для распознавания статистические данные. Кроме того, в обратной ситуации, когда начертание символов практически не изменяется от раза к разу — можно с уверенностью распознать данный символ уже после первого ввода (ситуация характерная только для печатного текста). Это приводит к необходимости использования в интерфейсе формирования статистик в рамках концепции обратной связи. Приложение должно оценивать полноту статистические данные и при накоплении достаточного количества статистических данных переходить к следующему символу.

В свою очередь при рассмотрении символов не вырванными из контекста, а в составе сложного рукописного текста можно видеть, что начертание символов зависит не только от простых случайных изменений при написании, но и от предыдущего и последующего символа в слове. Форма символов изменяется в различных комбинациях и соседние буквы (соединения с соседними буквами) очень сильно влияют на форму текущей букв. Иными словами мы сталкиваемся с необходимостью, кроме сбора частных статистик на отдельно стоящие буквы, проводить тот же процесс и для комбинаций символов.

Однако запрашивать у пользователя начертание каждой возможной комбинации символов, да еще и не менее трех раз, просто нежелательно. Для экономии ресурсов пользователя имеет смысл разработка специального текста для рукописного ввода в программу. Этот текст должен содержать минимальный набор символов и комбинаций для формирования статистик рукописного воспроизведения букв пользователем.

Этот текст, написанный пользователем, разбивается на символы и комбинации символов, используемые для формирования статистик. При недостатке данных необходимо, в целях экономии ресурсов пользователя, применять интерполяцию уже собранных данных для получения промежуточных вариантов ввода.

Допустим, было проведено три запроса данных, в результате чего программой были получены статистические данные $\{X_1(t);Y_1(t)\}$, $\{X_2(t);Y_2(t)\}$, $\{X_3(t);Y_3(t)\}$. После приведения к единому масштабу, для расширения обучающей выборки, над данными проводится линейный морфинг, в результате которого мы получаем $(N-1)!*M^2$ образцов для обучения, где N - количество вводов пользователя, а M — плотность выборки морфинга. Это позволяет существенно сократить затраты пользователя на обучение нейронной сети.

Важно понимать, что от плотности выборки морфинга напрямую зависит качество обучения нейронной сети. При слишком частой выборке, образцы для обучения будут иметь мало различий друг от друга. С другой стороны, при слишком редкой выборке снижается количество получаемых данных и возрастает нагрузка на пользователя. На рисунке 2 показана схема проведения морфинга между получаемыми образцами.

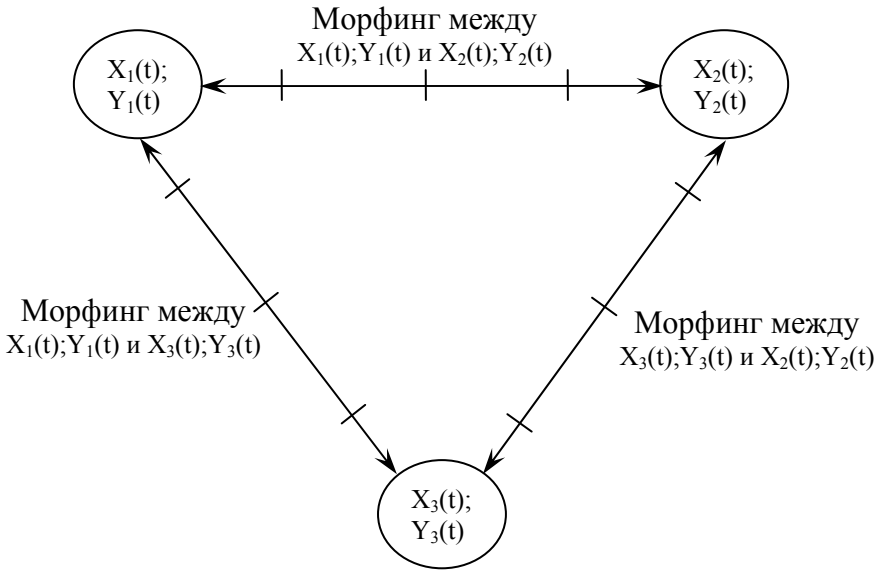


Рисунок 2. Морфинг введенных данных.

Алгоритму распознавания, использующемуся в программе, для оптимального обучения необходимо порядка 12 -16 примеров. Для их получения из введенных данных необходимо использовать сбалансированную стратегию получения образцов для обучения из введенных данных и данных полученных с помощью морфинга.

После анализа основного текста и оценки собранной информации возможен запрос у пользователя повторного ввода тех символов и комбинаций, по которым не был достигнут удовлетворительный уровень распознавания. С использованием морфинга при каждом последующем вводе данных будут учитываться не только введенные, но и результаты морфинга с уже введенными образцами.

Такая оптимизация интерфейса пользователя позволяет избавиться от ввода каждого символа и формировать статистики по введенному тексту и проводить гибкий анализ статистических данных, экономя при этом ресурсы пользователя и не загружая его однообразным вводом.

Литература:

1. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза - 2005г. Издательство Пензенского государственного университета, 273 с.

2. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

Получено 25.11.2007 г. Опубликована в Интернет 1.12.2007.

СОДЕРЖАНИЕ

Труды научно-технической конференция
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Том 7
Пенза – 2007 г.

ЛР № 020779

Подписано к печати 18.05.2008 г.
Тираж 200 экз.
Усл. печ. л. 4,75.

Формат 60x84 1/16

Технический редактор А.Н. Шумаров
(841-2)63-81-15, 63-80-44

Издательство Пензенского научно-исследовательского
электротехнического института
440601, г. Пенза, ул. Советская, 9.

Отпечатано с готового оригинал-макета в информационно-издательском центре
Пензенского государственного университета. Заказ №
Бумага писчая № 1. Печать – RISO.
Пенза, Красная 40, т.: 52-47-33