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 6

Пенза 2005

УДК: 681.322

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Труды научно-технической конференции под редакцией Волчихина В.И., Зефирова С.Л.. – Пенза – декабрь – 2005. Издательство Пензенского научно-исследовательского электротехнического института. Том 6. 102 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 августа по декабрь 2005 года. Том 6 содержит 22 статью, отражающие точку зрения 28 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.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.3-4. Секция-2: Информационная безопасность сложных систем
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/001)

ОЦЕНКА ИЗБЫТОЧНОСТИ НЕЙРОСЕТЕВЫХ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИИ В БИНАРНЫЙ КОД

Хозин Ю.В., Надев Д.Н., Захаров О.С., Иванов А.И.
Лаборатория биометрических и нейросетевых технологий
Пензенского научно-исследовательского электротехнического института

В настоящее время активно развивается технология высоконадежной биометрико-нейросетевой аутентификации. Используются большие нейронные сети, обученные преобразовывать рукописный образ в бинарный код ключа (длинного пароля). Очевидно, что эти же технологии могут быть использованы и для распознавания рукописных букв конкретного пользователя. Пример экранной формы нейросетевого распознавателя рукописных букв приведен на рисунке 1.

Завышенные требования, предъявляемые к высоконадежным нейросетевым преобразователям биометрии в бинарный код [1], обусловлены тем, что нейросетевой преобразователь должен иметь равновероятные характеристики («0», «1») на каждом из его бинарных выходов. Это необходимо для того, чтобы сделать неэффективным статистический нейрокриптоанализ. Однако, столь жесткие требования, как правило, приводят к снижению вероятностных характеристик систем распознавания. Так однослойная искусственная нейронная сеть с 88 входами, 256 выходами (каждый нейрон имеет 25 входов) дает коллизии при распознавании некоторых образов. В частности, такая сеть, обученная распознавать образ «a», достаточно часто дает коллизии с образом «n» и образом «c» (см. рисунок 1).

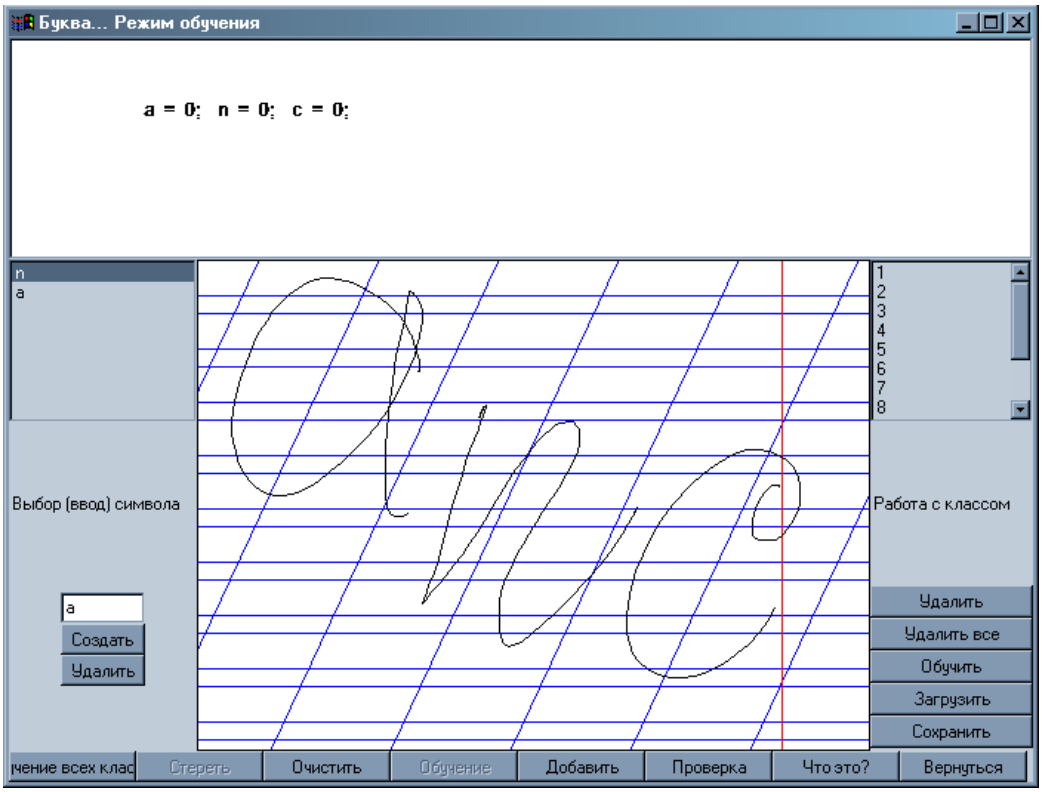

Рисунок 1 – Экранная форма нейросетевого распознавателя рукописных букв, дающего при распознавании коллизии образов «a», «n», «c».

Вероятность ошибочного принятия образа «n» за образ «a» составляет 0,7. Вероятность ошибочного принятия образа «c» за образ «a» составляет 0,55. Вероятность ошибочного принятия образа «c» за образ «n» составляет 0,65.

Коллизии обусловлены тем, что образы «a», «c», «n» имеют распределение значений с одним знаком (см. рисунок 2).

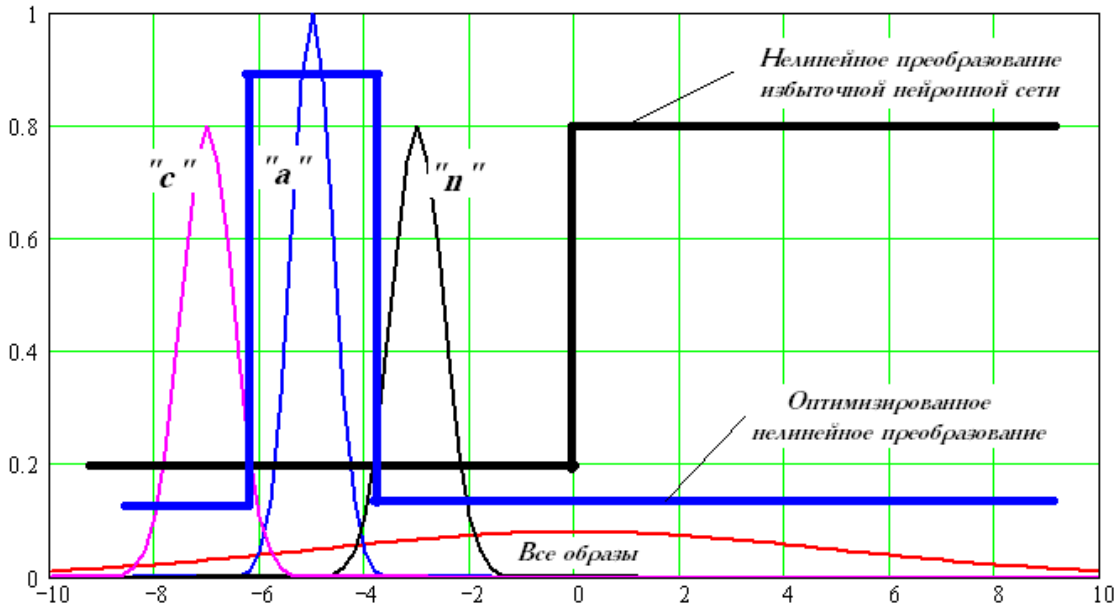

Рисунок 2 – Пример распределения значений, соответствующих разделяемым классам на выходе одного из нейронов, иллюстрирующий эффект коллизии.

Избавиться от коллизий можно, оптимизировав вид нелинейности на выходе нейронов. При этом мы теряем равную вероятность выходных состояний бинарных выходов нейросетей, но существенно повышаем качество распознавания. На рисунке 2 оптимизированное нелинейное преобразование нейрона дает вероятность 0.1 появления значения «1» и вероятность 0.9 появления значения «0». Качество решения существенно увеличивается.

В том случае, если состояние «1» имеет ширину в 3 дисперсии относительно центра распределения образов «a», вероятность коллизий с «n» уменьшается до значения 0,012. Мы имеем почти 60-кратное уменьшение вероятности ошибочного возникновения коллизий. При аналогичном вычислении для образов «c», «a» вероятность коллизий уменьшается до значения 0,003, что соответствует почти 200-кратному снижению вероятности ошибки.

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.

Получено 16.08.2005. Опубликовано в Internet 20.12.2005

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.5-7. Секция-2: Информационная безопасность сложных систем.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/002)

ОЦЕНКА ПОТЕНЦИАЛЬНОЙ ИНФОРМАТИВНОСТИ НЕЙРОПРЕОБРАЗОВАНИЯ БИОМЕТРИЧЕСКОГО ОБРАЗА В КРИПТОГРАФИЧЕСКИЙ КЛЮЧ ДОСТУПА

Иванов А.И., Малыгин А.Ю., Семенов А.В.

Проект первой редакции национального российского стандарта по требованиям к средствам высоконадежной биометрии [1] делит все биометрические средства по их стойкости к атакам подбора на сильные и слабые. При этом в приложении «А» к стандарту даны рекомендуемые длины ключей доступа для разнотипных биометрических средств защиты, сбалансированных по стойкости к атакам на биометрию и криптографию.

При атаке подбора на биометрию и криптографию предполагается, что злоумышленник имеет программное обеспечение механизма защиты, включающее проверку правильности преобразования биометрия-код ключа доступа. В связи с этим злоумышленник может реализовать автоматизированную атаку подбора биометрических данных на входе нейропреобразователя или его действительного выходного криптографического ключа.

Атака подбора криптографического ключа должна осуществляться, исходя из гипотезы равновероятности состояний каждого его разряда и отсутствия заведомо слабых ключевых комбинаций. Например, может быть использован направленный перебор всех сильных ключевых состояний, что в свою очередь может потребовать значительных вычислительных ресурсов. Предположительно злоумышленник не будет атаковать криптографические механизмы защиты и сам криптографический ключ, заведомо зная о высокой стойкости классических криптоалгоритмов.

Отказавшись от атак на криптографию, с высокой вероятностью злоумышленник будет атаковать биометрические механизмы защиты, надеясь найти в них брешь. Для организации эффективной атаки подбора биометрических данных злоумышленнику необходимо иметь статистику распределения значений контролируемых механизмом защиты биометрических параметров всех возможных биометрических образов. Для сбора статистики достаточно подать на вход взламываемой биометрической системы несколько сот однотипных биометрических образов и, контролируя каждый из входов нейросетевого преобразователя, рассчитать необходимое число статистических моментов. Подобные статистические исследования упрощаются тем, что, как правило, контролируемые биометрические параметры имеют нормальный закон распределения, а при предварительной обработке биометрических данных зачастую осуществляется их центрирование. Тогда злоумышленнику необходимо определить только вектор дисперсий контролируемых биометрических параметров. Блок-схема предварительных статистических исследований биометрического механизма защиты приведена на рисунке 1.

Исходя из вышеизложенного, можно предполагать, что подготовленный злоумышленник всегда будет иметь полную информацию о векторе дисперсий контролируемых той или иной системой защиты биометрических параметров.

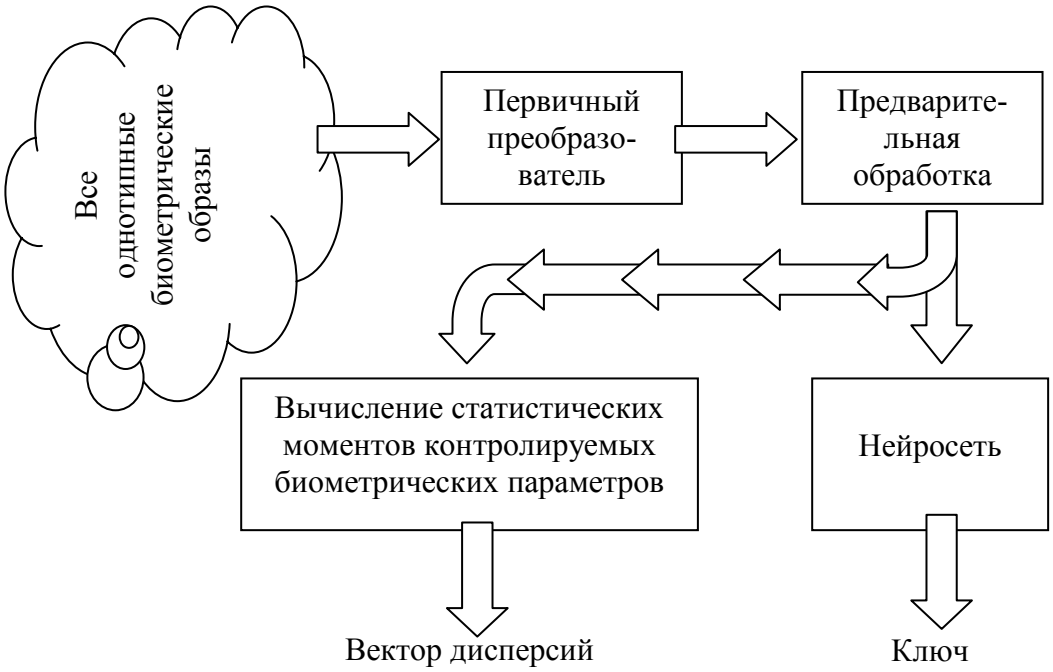

Рисунок 1 – Блок-схема проведения статистического исследования биометрического механизма защиты.

Располагая вектором дисперсий контролируемых биометрических параметров, злоумышленник имеет возможность организовать достаточно эффективную атаку их перебора. Блок-схема организации такой атаки отображена на рисунке 2.

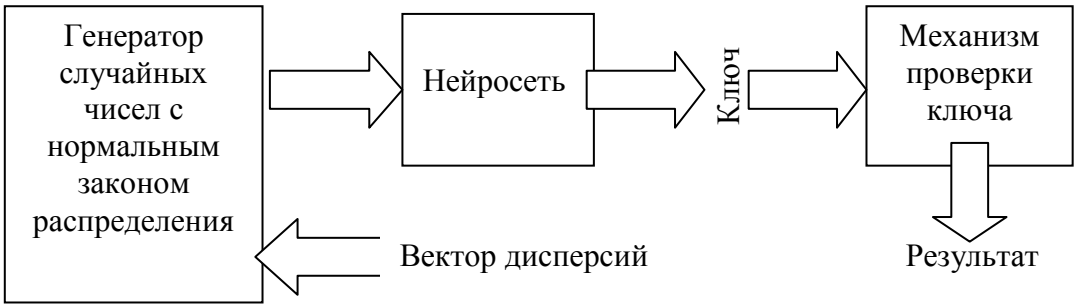

Рисунок 2 – Блок-схема организации атаки подбора биометрических параметров механизма защиты

Результат атаки подбора, организованной в соответствии с блок-схемой рисунка 2, можно наблюдать, используя имеющийся в биометрической защите механизм проверки ключа. Как правило, в программе биометрической защиты хранится хэш-функция правильного ключа для промежуточной проверки результатов нейросетевого преобразования. Соответственно, злоумышленник потенциально способен извлечь из программы биометрической защиты значение контрольной хэш-функции и, зная его, организовать контроль результатов перебора.

Следует подчеркнуть, что приведенная выше схема носит иллюстративный характер и вряд ли будет использована для атаки на реальные механизмы высоконадежной биометрической защиты. Эта схема атаки не имеет памяти об

уже проверенных возможных комбинациях биометрических параметров и, следовательно, неэффективна из-за возможных многократных повторений. Видимо, реальные атаки на биометрию должны организовываться по иной схеме.

Приведенная выше схема полезна тем, что позволяет оценивать информативность уже обученной на конкретный биометрический образ защиты. При тестировании защиты мы знаем все значения биометрических параметров. Как следствие мы можем часть подбираемых параметров считать известными и тем самим ослабить систему защиты до доступного для реального тестирования уровня. Далее по блок-схеме рисунка 2 осуществляется подбор оставшихся неизвестными параметров и подсчитывается ушедшее на подбор число попыток. Учитывая, что биометрические параметры имеют разное качество, целесообразно многократно повторить результаты тестирования. Итоги тестирования усредняются для одинаково ослабленного механизма защиты.

Описанная выше методика тестирования высоконадежных биометрических механизмов защиты в конечном итоге позволяет оценивать стойкость защиты или их потенциальную информативность. Практика показывает, что чем больше информации имеет тот или иной биометрический образ (чем он сложнее), тем труднее его подбирать. Например, простой отпечаток пальца, имеющий только 16 особых точек, имеет эквивалентную по стойкости к атакам подбора длину ключа 17 бит [1]. Более сложный отпечаток пальца с 38 особыми точками соответствует более длинному криптографическому ключу из 39 бит с большей стойкостью к атакам подбора. Таким образом, тестирование обученного механизма защиты по блок-схеме рисунка 2 позволяет оценивать информативность любых биометрических образов и прогнозировать стойкость этих механизмов защиты к атакам подбора или полного перебора.

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.

Получено 15.11.2005. Опубликовано в Internet 20.12.2005

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.8-9. Секция-9: Аутентификация: парольная, биометрическая, криптографическая
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/003)

ОЦЕНКА АДДИТИВНОЙ ПОГРЕШНОСТИ ЗАМЕНЫ БИНОМИАЛЬНОГО ЗАКОНА РАСПРЕДЕЛЕНИЯ НА НОРМАЛЬНЫЙ ЗАКОН ПРИ ИССЛЕДОВАНИЯХ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ/КОД КЛЮЧА ДОСТУПА

Надев Д.Н., Иванов А.И.

Проект первой редакции национального российского стандарта по требованиям к средствам высоконадежной биометрии [1] предполагает использование преобразователей биометрия/код высокой размерности. Подобные преобразователи могут быть построены с использованием искусственных нейронных сетей, либо с использованием нечетких функций [2]. Независимо от технологии расчета таких преобразователей на их выходах разряды бинарного кода должны быть некоррелированы и иметь равновероятное значение состояний «0», «1» для входных случайных образов «Все чужие». Проведенные исследования подобных преобразователей показали, что выходная последовательность кодов, соответствующая случайным входным биометрическим образам «Все чужие», с высокой точностью соответствует нормальному закону распределения значений меры Хемминга или расстояния между заданным кодом «Свой» и случайными выходными кодами «Все чужие». Такая ситуация характерна для случая, когда «Чужой» ничего не знает о подбираемом им биометрическом образе и вынужден предъявлять преобразователю случайные образы.

Ситуация меняется, когда «Чужой» частично или полностью скомпрометировал биометрический образ «Свой». Тогда наблюдается явная асимметрия закона распределения значений (первый и третий моменты существенно отличаются от ноля).

Эффект полной симметрии закона распределения и его абсолютно точного совпадения с нормальным законом (при $p = 0{,}5$), а также эффект отсутствия симметрии p, хорошо описывается биномиальным законом распределения значений. Примеры плотностей распределения биномиального закона распределения, превращающегося в нормальный закон при $p = 0.5$, приведены на рисунке 1.

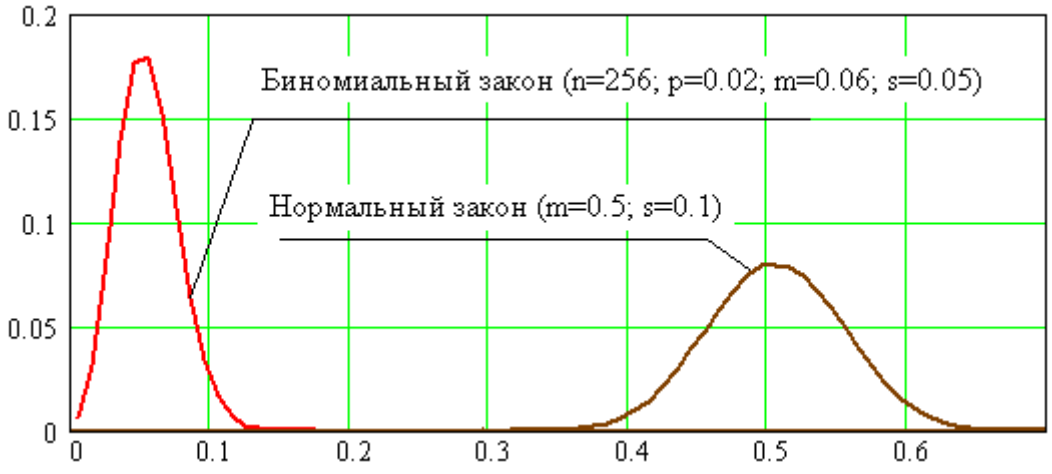

Рисунок 1 – Биномиальный закон распределения значений при равновероятном и не равновероятном значениях состояний «0», «1» разрядов выходного кода

Очевидно, что по мере увеличения компрометации входной биометрической информации асимметрия выходных распределений будет расти. Пример этого эффекта приведен на рисунке 2, где видно, что нормальный закон может иметь отрицательные расстояния Хемминга, в то время как технически и по биномиальному закону это невозможно.

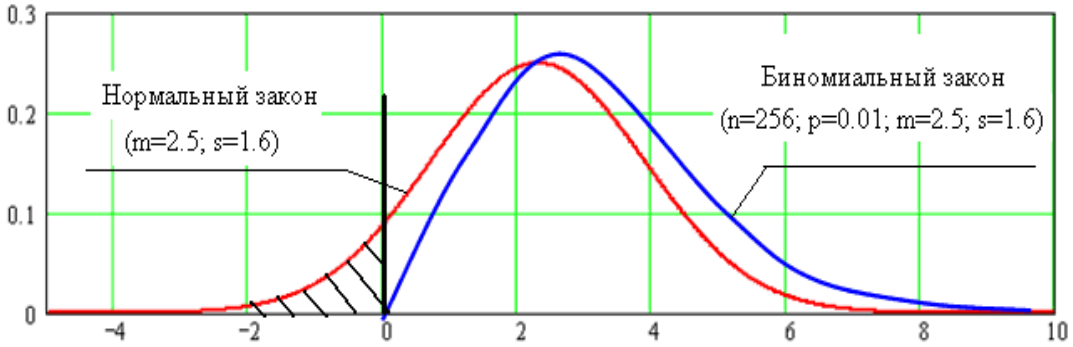

Рисунок 2 – Эффект появления отрицательных значений меры Хемминга при замене биномиального распределения нормальным законом распределения

Казалось бы эффект отображенный на рисунке 2 исключает возможность замены биномиального распределения нормальным, однако это далеко не так. Численные эксперименты показали, что биномиальный закон и нормальный закон распределения значений близки и вполне заместимы. Возникающая при этом аддитивная приведенная ошибка не превышает -20%, монотонна и может быть легко скорректирована. График ошибки дан на рисунке 3.

Рисунок 3 - Значение аддитивной приведенной погрешности в зависимости от значения математического ожидания относительной меры Хемминга

Для корректировки ошибки достаточно вычислить среднее значение относительной меры Хемминга, найти по нему величину приведенной аддитивной ошибки по графику рисунка 3 и уменьшить на ее значение вероятность, рассчитанную в рамках гипотезы нормального закона распределения.

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. Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data /Yevgeni Dodis, Leonid Reyzin, Adam Smith //April 13, 2004. www.cs.bu.edu/~reyzin/fuzzy.html

Получено 15.11.2005. Опубликовано в Internet 20.12.2005

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.10-12. Секция-5: Управление информационной безопасностью
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/004)

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ФАЗОВОЙ СИНХРОНИЗАЦИИ С РАВНОМЕРНОЙ ДИСКРЕТИЗАЦИЕЙ ТРЕТЬЕГО ПОРЯДКА

Дорошкевич В.В. E-mail: ibst@stup.ac.ru
Пензенский государственный университет

Объектом исследования являются системы фазовой синхронизации (СФС) с равномерной дискретизацией (РД) [1], которые представляют собой дискретные аналоги цифровых СФС с аналого-цифровым преобразователем (АЦП) до контура регулирования, получаемые в предположении бесконечной разрядности АЦП. Подобные системы используются при когерентном приёме сигналов с различными видами модуляции в составе разнообразных устройств техники связи, применяемых в защищённых телекоммуникационных системах (в частности, при построении цифровых модемов и эхокомпенсаторов [2]), а также в измерительно-вычислительных комплексах (например, для оценки параметров гармонического колебания, наблюдаемого на фоне шума [3]) и т.д. В работе [1] была построена обобщенная математическая модель СФС данного класса, иллюстрируемая схемой на рисунке 1.

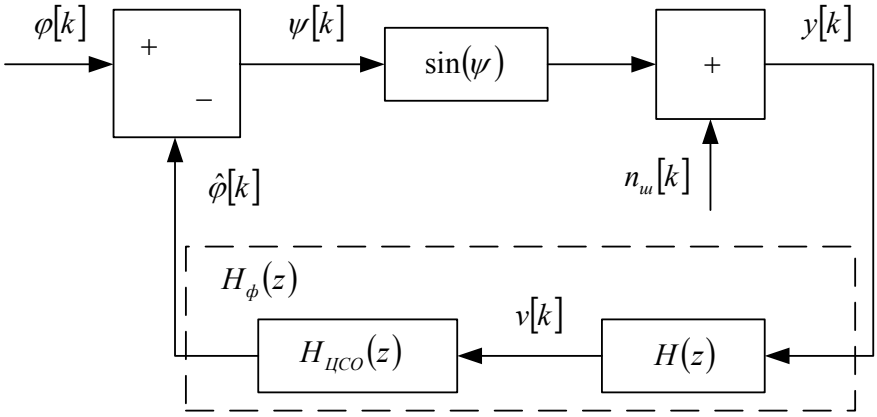

Рисунок 1

Модель включает в себя фазовый дискриминатор (ФД) с синусоидальной нелинейностью, выделяющей разность фаз $\psi[k]$ задающего $\varphi[k]$ и подстраиваемого $\hat{\varphi}[k]$ колебаний и изображенной на рисунке в виде трёх верхних блоков, а также эквивалентный петлевой фильтр с передаточной функцией $H_{\phi}(z)$. Как видно из рисунка,

$$H_{\Phi}(z) = H(z)\, H_{\text{ЦСО}}(z), \qquad (1)$$

где $H_{\text{ЦСО}}(z) = z^{-1}/(1 - z^{-1})$ – комплексный коэффициент входящего в состав СФС цифрового синтезатора отсчетов подстраиваемого колебания; а $H(z)$ – передаточная функция цифрового фильтра СФС, определяющего порядок и свойство этой системы.

Одним из известных вариантов построения ЦФ, применяемых в СФС, является выполнение его в виде структур, изображенных на рисунках 2а и 2б.

Причем фильтр, изображенный на рисунке 2а, соответствует СФС 2-го, а на рисунке 2б – СФС 3-го порядка (в системе 1-го порядка роль этого фильтра выполняет масштабирующий коэффициент β, входящий в состав верхней ветви на рисунках 2а и 2б) [4].

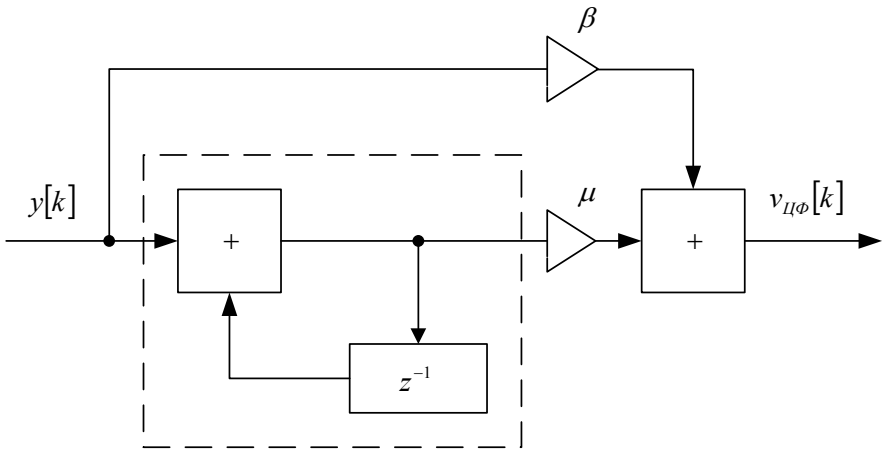

Рисунок 2а

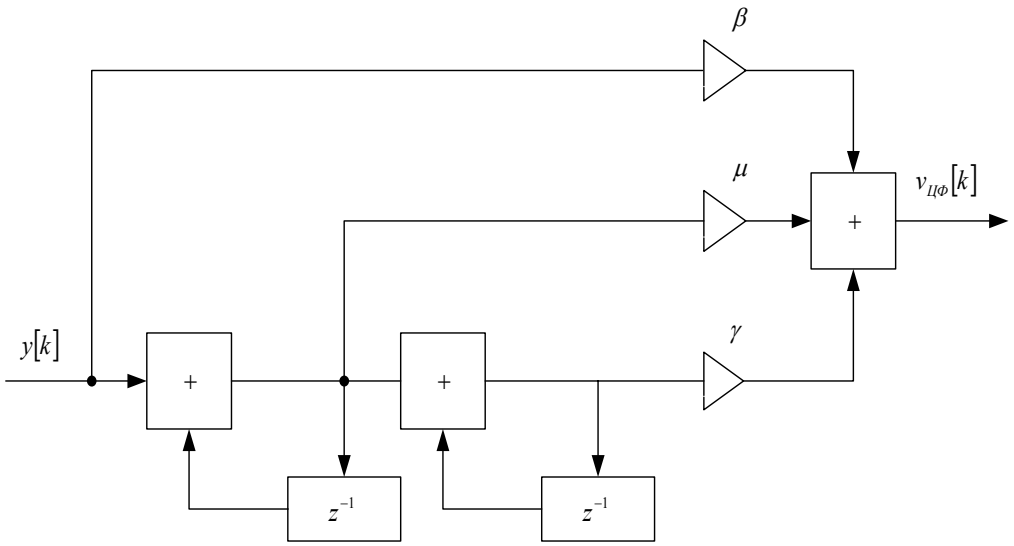

Рисунок 2б

В работе [1] было получено нелинейное разностное уравнение, цифровой СФС 2-го порядка, построенной с использованием фильтра, показанного на рисунке 2а. Решим аналогичную задачу для системы 3-го порядка с фильтром, изображённым на рисунке 2б.

Для этого, прежде всего, необходимо определить передаточную функцию ЦФЗ. Как видно из схемы, структура фильтра состоит из 3 параллельных ветвей: верхней с коэффициентом передачи $H_{ЗВ}(z) = \beta$; средней, включающей накапливающий сумматор и масштабирующий коэффициент μ; нижней, включающей два последовательно включенных накапливающих сумматора и масштабирующий коэффициент γ.

Учитывая, что комплексный коэффициент передачи накапливающего сумматора $H_{НС}(z)$ определяется соотношением [4]:

$$H_{НС}(z) = 1/(1 - z^{-1}),$$

для передаточных функций средней $H_{ÇÑÐ}(z)$ и нижней $H_{ÇH}(z)$ ветвей получаем следующие соотношения: $H_{ÇÑÐ}(z)=\mu/\left(1-z^{-1}\right)$ и $H_{ÇH}(z)=\gamma/\left(1-z^{-1}\right)^2$.

Результирующая системная функция ЦФЗ определяется как:

$$H(z)=H_{ЗВ}(z)+H_{ЗСР}(z)+H_{ЗН}(z)=\left[\beta z^{-2}-(2\beta+\mu)z^{-1}+\beta+\mu+\gamma\right]/\left(1-z^{-1}\right)^2 .$$

Подставляя полученный результат в (1), получаем:

$$H_{ф}(z)=H(z)\,H_{ЦСО}(z)=\frac{\beta z^{-3}-(2\beta+\mu)z^{-2}+(\beta+\mu+\gamma)z^{-1}}{\left(1-z^{-1}\right)^3}=\frac{k_3z^{-3}+k_2z^{-2}+k_1z^{-1}}{1-3z^{-1}+3z^{-2}-z^{-3}},$$

где $k_1=\gamma+\mu+\beta$, $k_2=-(2\beta+\mu)$, $k_3=\beta$.

Передаточной функции $H_{ф}(z)$ соответствует временной алгоритм:

$$\hat{\varphi}[k]=3\hat{\varphi}[k-1]-3\hat{\varphi}[k-2]+\hat{\varphi}[k-3]+k_1y[k-1]+k_2y[k-2]+k_3y[k-3] \qquad (2)$$

Как показано в работе [1], выходной сигнал ФД $y[k]$ определяется выражением:

$$y[k]=\sin\psi[k]+n_{ш}[k], \qquad (3)$$

где $n_{ш}[k]$ – отсчеты дискретного белого гауссовского шума с дисперсией $\sigma_{ш}^2=\sigma^2/2U^2$; σ^2 – дисперсия входного белого гауссовского шума; $\sqrt{2}U$ – амплитуда задающего гармонического колебания на входе СФС.

Учитывая вытекающие из рисунка 1 соотношения $\psi[k]=\varphi[k]-\hat{\varphi}[k]$ и подставляя (3) в (2), получаем математическую модель СФС 3-го порядка в виде нелинейного разностного уравнения:

$$\psi[k]-3\psi[k-1]+3\psi[k-2]-\psi[k-3]+k_1\sin\psi[k-1]+k_2\sin\psi[k-2]+k_3\sin\psi[k-3]=$$
$$=\varphi[k]-3\varphi[k-1]+3\varphi[k-2]-\varphi[k-3]-k_1n_{ø}[k-1]-k_2n_{ø}[k-2]-k_3n_{ø}[k-3].$$

Полученные результаты могут служить основой для анализа характеристик рассмотренного класса СФС.

ЛИТЕРАТУРА:

1. *Султанов Б.В, Щербаков М.А., Захаренков В.Е., Дорошкевич В.В.* Математические модели цифровых систем фазовой синхронизации с равномерной дискретизацией // Доклады 4-й Международной Конференции «Цифровая обработка сигналов и ее применения». – М., 27 февраля – 1 марта 2002. – Т. 1 – С.106 – 109.
2. *Бочков В.К.* и др. Двухпроводный дуплексный модем // Электросвязь. – 2000. – № 7. – С. 35 – 38.
3. *Султанов Б.В.* Применение цифровых систем фазовой синхронизации для измерения сдвига частоты гармонического сигнала на фоне шума // Радиотехника. – 2000. – № 9. – С. 21 – 26.
4. *Линдсей У.Ч., Цзе Цзамин.* Обзор цифровых систем фазовой автоподстройки частоты // ТИИЭР. – 1981. – Т. 69. – № 4. – С. 12 – 33.

Получено 29.11.2005. Опубликовано в Internet 20.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.13-15. Секция-9: Аутентификация: парольная, биометрическая, криптографическая
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/005)

КОНТРОЛЬ РАБОТОСПОСОБНОСТИ МЕХАНИЗМА ЦЕНТРИРОВАНИЯ ВХОДНЫХ ДАННЫХ ПРЕОБРАЗОВАТЕЛЯ БИОМЕТРИЯ / КОД

Захаров О.С., Надеев Д.Н., Иванов А.И., Тришин А.В.

Проект первой редакции национального российского стандарта по требованиям к средствам высоконадежной биометрии [1] предполагает использование преобразователей биометрия/код высокой размерности. Подобные преобразователи могут быть построены с использованием искусственных нейронных сетей либо с использованием нечетких функций [2]. Независимо от технологии расчета таких преобразователей на их выходах разряды бинарного кода должны быть некоррелированы и иметь равновероятное значение состояний «0», «1» для входных случайных образов «Все чужие». Распределения значений меры Хемминга отклонений выходных кодов «Все чужие» от кода «Свой» имеют биномиальный закон распределения. По требованиям стандарта [1] математическое ожидание меры Хемминга отклонения случайных выходных кодов должно быть близко к половине длины ключа. Для нейросетевых преобразователей биометрия/код значение математического ожидания выходных кодов существенно зависит от корректности выполнения операции центрирования входных биометрических данных. Как следствие, необходим контроль работоспособности механизма центрирования.

Для примера рассмотрим контроль механизма центрирования демонстрационной версии преобразователя биометрия/код «Нейрокриптон». Проверку будем осуществлять на трех рукописных образах, примеры написания которых приведены на рисунке 1.

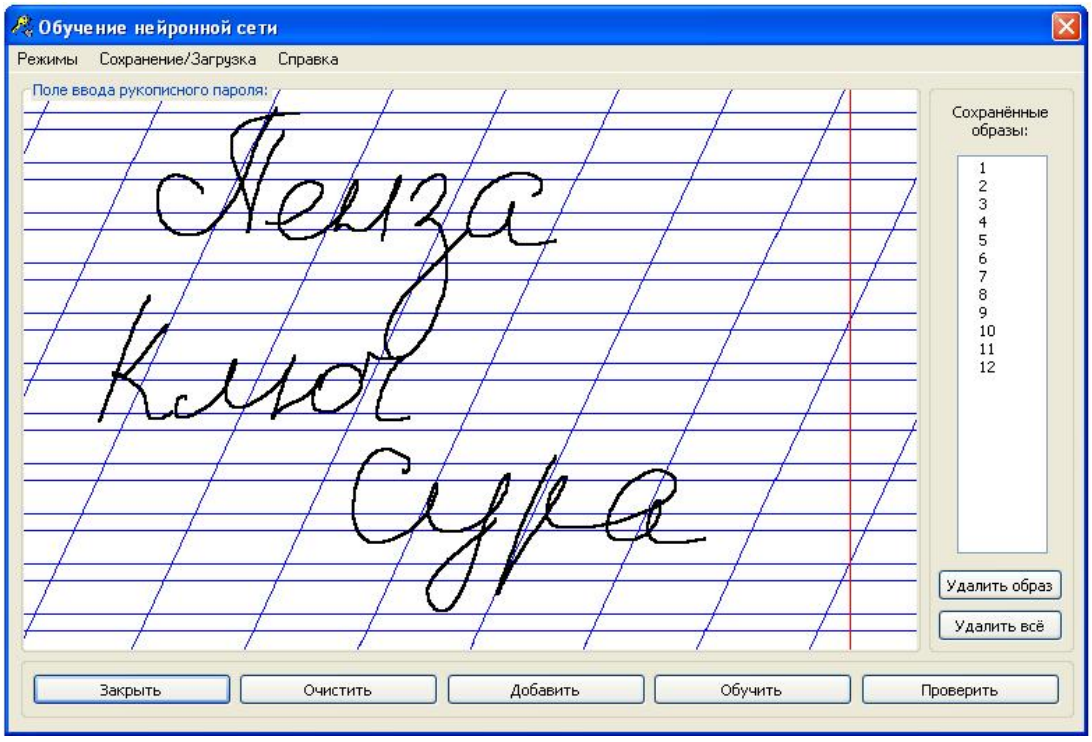

Рисунок 1 – Экранная форма ввода рукописных образов при обучении преобразователя биометрия/код «Нейрокриптон»

Демо-версия программы «Нейрокриптон» была обучена на каждом из приведённых выше образов (обучение осуществлялось на 12 примерах). После этого вводились случайные рукописные образы. В программном обеспечении хранителя паролей «Нейрокриптон» предусмотрена электронная форма проверки полученного ключа (осуществляется сравнение с эталоном). На рисунке 2 приведена экранная форма, отображающая поразрядно правильность полученного ключа. Несовпавшие биты ключа отображаются звёздочками, общее количество несовпавших бит (мера Хемминга) отображается в поле вывода, сообщающем о результате аутентификации.

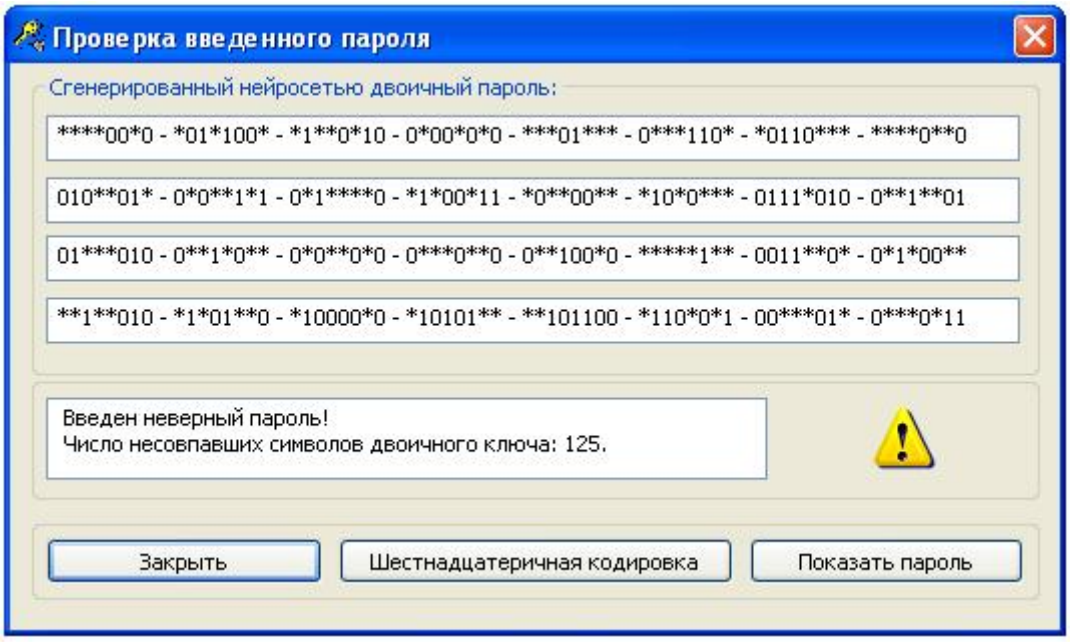

Рисунок 2 – Экранная форма ввода выходного кода, полученного при рукописном вводе случайного рукописного слова

Тестирование каждого из биометрических рукописных образов осуществлялось на 100 случайных рукописных образах «Чужой». Распределение меры Хемминга отклонения случайного кода «Чужой» от заданного кода «Свой» хорошо описывается нормальным законом. Результаты тестирования представлены на рисунке 3. Толстыми линиями отображены плотности распределения, полученные при тестировании программного обеспечения с включённым механизмом центрирования входных данных. Как видно из рисунка 3, математические ожидания правильно центрированных плотностей распределения образов «Свой» близки к половине длины ключа – 128 битам.

Результаты тестирования программного обеспечения с отключенным механизмом центрирования отображены на рисунке 3 тонкими линиями. Как видно из рисунка, математические ожидания нецентрированных плотностей распределения образов «Свой» смещаются влево. Ошибки из-за неправильного центрирования (Δ_1, Δ_2, Δ_3) примерно одинаковы и составляют 42 бита. В связи с тем, что дисперсия у правильно центрированных и смещённых плотностей распределения примерно одинакова, потери от неправильного смещения для тестируемой системы будут составлять 1 – 2 порядка.

Из приведённого рисунка 3 видно, что результаты тестирования существенно зависят от особенностей используемого рукописного слова. В связи с этим корректное тестирование может быть осуществлено на 20 – 30 различных словах. То есть, представительная выборка образов «Чужой» должна быть не менее 100, а представительная выборка «Свой» должна быть не менее 20.

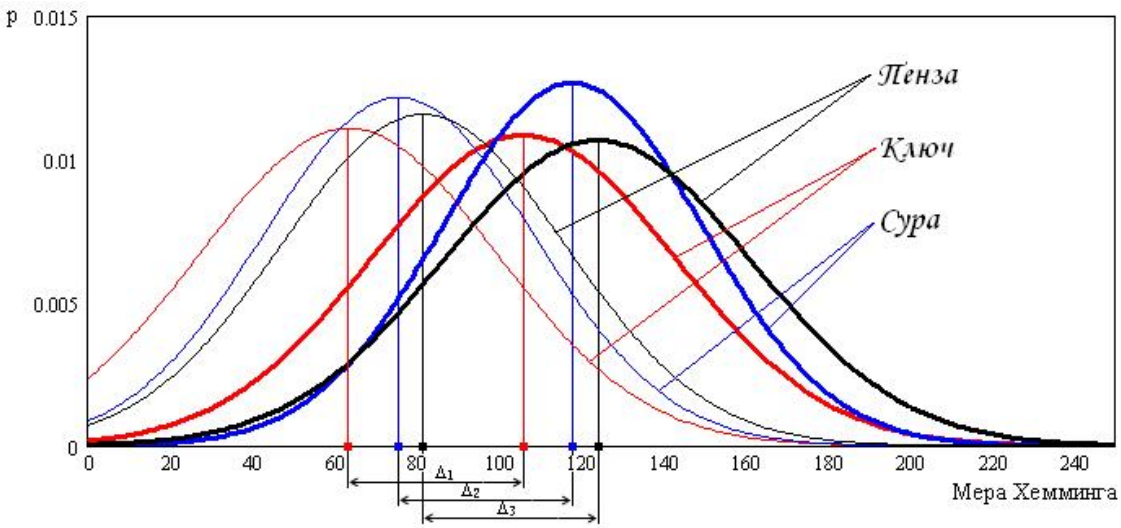

Рисунок 3 – Смещение распределений образов «Все чужие» для разных парольных слов с центрированием и без центрирования

Крайне желательным является сбалансированность используемых тестовых выборок. Небольшие тестовые выборки должны быть корректно сбалансированы и правильно отражать свойства статистических моментов генеральной совокупности.

Объём приведённых выше тестовых испытаний невелик, и с ними может справиться любой производитель, однако мелкие производители будут получать корректные результаты тестирования только при наличии сбалансированных тестовых выборок. Создание эталонных тестовых выборок должно осуществляться силами специализированных центров. Желательно, чтобы все производители имели свободный доступ к эталонным тестовым выборкам малых размеров.

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. Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data /Yevgeni Dodis, Leonid Reyzin, Adam Smith //April 13, 2004. www.cs.bu.edu/~reyzin/fuzzy.html

Получено 05.12.2005. Опубликовано в Internet 20.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.16-18. Секция-5: Управление информационной безопасностью
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/006)

АЛГОРИТМ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ СИСТЕМЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В РЕАЛЬНОМ ВРЕМЕНИ

Машкина И.В., Рахимов Е.А., Дивель А.В. E-mail: Gin2003@km.ru
Уфимский государственный авиационный технический университет

Разработка систем управления защитой информации является актуальным направлением обеспечения безопасности объектов информатизации, функционирующих в условиях информационного противоборства.

Под управлением защитой информации понимается возможность изменения технологии обработки информации, усиление функций системы защиты информации (СЗИ), переконфигурация СЗИ на основе анализа данных о внешних воздействиях и состоянии защищаемой информационной системы.

Система управления (СУ) защитой информации оценивает и анализирует динамическое изменение пространства информационных угроз, состояние СЗИ и реагирует на эти изменения, обеспечивая требуемый уровень защищенности объекта информатизации. Одним из основных элементов подсистемы принятия решений СУ является оперативный решатель, позволяющий системе производить выбор оптимальных управляющих воздействий на СЗИ.

Одной из задач по переконфигурации СЗИ является задача выбора используемых антивирусных программ.

В настоящее время известно большое число антивирусных программ, которыми может воспользоваться администратор безопасности в случае обнаружения аномальной активности на объекте информатизации.

Для усиления функций защиты администратор безопасности может подключить дополнительно одну из антивирусных программ.

Алгоритм выбора набора из двух антивирусов реализуется программно. Одновременно возможно использовать только два антивируса, так как использование большего числа антивирусных пакетов приводит к перегрузке системных ресурсов.

В данной работе рассматривается возможность использования алгоритма принятия решений в условиях риска [1] для выбора оптимального набора антивирусных программ, который должен автоматически выполняться в оперативном решателе СУ. Предварительно администратором должна быть выполнена работа по оценке совместимости антивирусных пакетов. В отличие от известного метода принятия решений в условиях статистической неопределенности [1], в котором вероятности альтернатив определяются, исходя из статистических данных, в рассматриваемой задаче вероятности альтернатив рассчитываются, а сами альтернативы представляют собой сочетание из двух элементарных альтернатив более низкого порядка.

Введем обозначения: первый антивирус обозначим A_1; второй антивирус – A_2; третий – A_3.

Из имеющихся статистических данных антивирус A_1 позволяет обнаруживать вновь появляющиеся вирусы с вероятностью P_1; A_2 – с вероятностью P_2; A_3 – с вероятностью P_3. Источниками статистических данных служат журналы работы антивирусов и данные, формируемые независимыми источниками.

Таким образом, имеется три альтернативы – X_1, X_2, X_3 и два исхода – Y_1, Y_2: X_1 – использование A_1 и A_2; X_2 – использование A_2 и A_3; X_3 – использование A_1 и A_3; Y_1 – вирус обнаружен; Y_2 – вирус не обнаружен.

Построим для данной задачи граф связи альтернатив и исходов (рисунок 1).

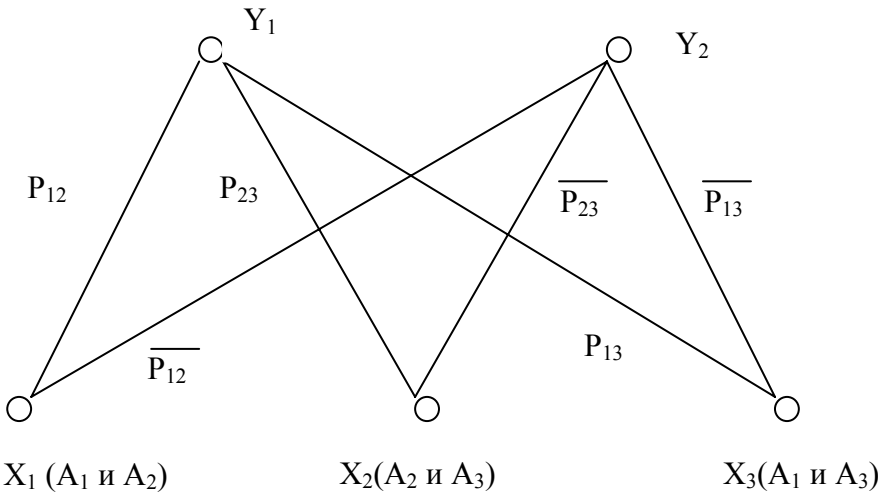

Рисунок 1 – Граф связи альтернатив и исходов

Рассчитаем вероятности наступления исходов. Два события: обнаружение вируса антивирусным пакетом A_i и антивирусным пакетом A_j – являются независимыми друг от друга, поэтому вероятность обнаружения вируса в случае одновременного использования пакетов может быть вычислена по формуле [3]:

$$P_{ij} = P_i + P_j - P_i \cdot P_j,$$

где Pi – вероятность обнаружения вируса при использовании пакета Ai, Pj – вероятность обнаружения вируса при использовании пакета Aj.

Вероятность того, что вирус не будет обнаружен комбинацией *i*-го и *j*-го средства, вычисляется как

$$\overline{P}_{ij} = (1 - P_i)(1 - P_j),$$

т.е. P_i есть вероятность не срабатывания i-го и j-го антивируса одновременно.

В соответствии с используемым методом вводится понятие состояния среды *Z*. В решаемой задаче число состояний среды $Z = 8$ (определяется произведением числа стрелок, выходящих из каждой альтернативы). Рассчитаем вероятности для этих состояний:

Z1: $X1 \to Y1;\ X2 \to Y1;\ X3 \to Y1;\ P(Z_1) = P_{12} \cdot P_{23} \cdot P_{13};$

Z2: $X1 \to Y1;\ X2 \to Y1;\ X3 \to Y2;\ P(Z_2) = P_{12} \cdot P_{23} \cdot \overline{P}_{13};$

Z3: $X1 \to Y1;\ X2 \to Y2;\ X3 \to Y1;\ P(Z_3) = P_{12} \cdot \overline{P}_{23} \cdot P_{13};$

Z4: $X1 \to Y1;\ X2 \to Y2;\ X3 \to Y2;\ P(Z_4) = P_{12} \cdot \overline{P}_{23} \cdot \overline{P}_{13};$

Z5: $X1 \to Y2;\ X2 \to Y1;\ X3 \to Y1;\ P(Z_5) = \overline{P}_{12} \cdot P_{23} \cdot P_{13};$

Z6: $X1 \to Y2;\ X2 \to Y1;\ X3 \to Y2;\ P(Z_6) = \overline{P}_{12} \cdot P_{23} \cdot \overline{P}_{13};$

Z7: $X1 \to Y2;\ X2 \to Y2;\ X3 \to Y1;\ P(Z_7) = \overline{P}_{12} \cdot \overline{P}_{23} \cdot P_{13};$

Z8: $X1 \to Y2;\ X2 \to Y2;\ X3 \to Y2;\ P(Z_8) = \overline{P}_{12} \cdot \overline{P}_{23} \cdot \overline{P}_{13}.$

Таким образом, можно задать функцию реализации в виде следующей таблицы:

	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8
X_1	Y_1	Y_1	Y_1	Y_1	Y_2	Y_2	Y_2	Y_2
X_2	Y_1	Y_1	Y_2	Y_2	Y_1	Y_1	Y_2	Y_2
X_3	Y_1	Y_2	Y_1	Y_2	Y_1	Y_2	Y_1	Y_2

Решая задачу в терминах «выгоды», следует ввести следующую численную оценку исходов в баллах: Y_1 (вирус обнаружен) – B баллов, Y_2 (вирус не обнаружен) – 0 баллов.

Таблица функции реализации приобретает вид:

	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8
X_1	B	B	B	B	0	0	0	0
X_2	B	B	0	0	B	B	0	0
X_3	B	0	B	0	B	0	B	0

Вычислим функционалы $J(X_i, Z)$

$$J(X1, Z) = P(Z1) \cdot B + P(Z2) \cdot B + P(Z3) \cdot B + P(Z4) \cdot B;$$
$$J(X2, Z) = P(Z1) \cdot B + P(Z2) \cdot B + P(Z5) \cdot B + P(Z6) \cdot B;$$
$$J(X3, Z) = P(Z1) \cdot B + P(Z3) \cdot B + P(Z5) \cdot B + P(Z7) \cdot B.$$

Выбор наилучшей альтернативы по функционалу можно представить следующей формулой:

$$X_{\text{îïò}} = X\left(\arg\max\left(J_i\right)\right).$$

В результате использования предлагаемого алгоритма принятия решений обеспечивается расширение диапазона перекрытия вирусной активности и, следовательно, повышение эффективности функционирования СЗИ.

ЛИТЕРАТУРА:

1. Черноруцкий И.Г. Методы оптимизации и принятия решений: учебное пособие. – СПб.: Издательство «Лань», 2001. – 384 с.
2. Манита А.Д. Теория вероятностей и математическая статистика: Учебное пособие. – М.: Издат. отдел УНЦ ДО, 2001. – 120 с.
3. http://www.viruslist.com/ru/analysis – Аналитика вирусов.

Получено 12.12.2005. Опубликовано в Internet 20.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.19-23. Секция-5: Управление информационной безопасностью
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/007)

ОБЪЕДИНЕНИЕ СИГНАЛОВ ПОСЫЛОК НА ФИЗИЧЕСКОМ УРОВНЕ ПРИ РАЗНЕСЕННОМ ПРИЕМЕ

Егорова Н.А., Кашаев Е.Д. E-mail: kashaev@beda.stup.ac.ru
Пензенский государственный университет

Для повышения целостности и доступности данных в автоматизированных системах радиосвязи используется метод разнесенного приема [1]. В классическом варианте объединения информации на канальном уровне сигналы обрабатываются в устройстве преобразования сигнала (УПС). Значение *n*-го бита в *q*-ом канале разнесения $c`_{к\,q}(n)$ может принимать два значения: «0» и «1»

$$c`_{к\,q}(n) = \begin{cases} 0, & если \quad R(n) < 0 \\ 1, & если \quad R(n) \geq 0 \end{cases}, \qquad (1)$$

где R(n) – значение скаляра на выходе детектора. В декодере помехоустойчивого кода формируется m-ая кодовая комбинация $b`_{к\,q}(m)$

$$b`_{к\,q}(m) = \Psi\,(\boldsymbol{c}`_{\boldsymbol{к\,q}}(m))\,. \qquad (2)$$

В общем случае декодер формирует указание $\mu_{к\,q}(m)$ об обнаружении ошибки в *m*-ой кодовой комбинации кода

$$\mu_{к\,q}(m) = \begin{cases} 0, & если \quad \boldsymbol{S}(m) = 0 \\ 1, & если \quad \boldsymbol{S}(m) \neq 0 \end{cases}, \qquad (3)$$

которое передается в устройство объединения кодовых комбинаций канального уровня. Буквой ***S*** обозначен синдром, получаемый в результате выполнения алгебраической операции декодирования.

В устройстве объединения выполняется операция объединения кодовых комбинаций, в частном случае, операция принятия решения по мажоритарному правилу [2]

$$b`_{к}(m) = \sum_{q=1}^{Q} \mu_{к\,q}(m)\, b`_{к\,q}(m)\,. \qquad (4)$$

В этом случае необходимым условием для (4) является нечетное количество каналов разнесения.

В [3] описан способ восстановления формы аналогового сигнала посылок, который повышает доступность данных. Процедура восстановления создает предпосылки для объединения сигналов на физическом уровне до детектора. С учетом свойства выравнивания временных задержек при выполнении процедуры

восстановления и снятия рассинхронизации несущих частот УПС операцию объединения предлагается выполнять за счет суммирования значений отсчетов сигналов на длительности обрабатываемой посылки [4]. Возможны два основных варианта реализации процедуры объединения. Сначала рассмотрим способ объединения сигналов при пространственно разнесенном приеме, при котором две или более приемных радиостанций работают на одной несущей частоте и одновременно принимают один и тот же переданный сигнал, прошедший по одной и той же трассе. Так как процедура восстановления позволяет объединить в один главный луч энергию всех лучей канала, то возможен следующий подход. Сначала сигналы с выходов разнесенных приемных радиостанций $s_1(t)$, $s_2(t)$,…, $s_Q(t)$ складываются

$$s`(i) = \sum_{q=1}^{Q} s_q(i), \tag{5}$$

а затем суммарный сигнал s`(i) подвергается процедуре восстановления.

$$x`(i) = \boldsymbol{s}`(i) * \boldsymbol{h}_{\mathbf{ув}}(i, \Delta f). \tag{6}$$

При этом фазовые соотношения и временные задержки сигналов с разнесенных радиостанций не учитываются, так как суммарный сигнал будет рассматриваться как сигнал, прошедший через один радиоканал с параметрами, соответствующими суммарной многолучевости. Структурная схема объединения изображена на рисунке 1. На рисунке 1 обозначено: РСТ – приемная радиостанция; УО – устройство объединения; УВ – устройство восстановления.

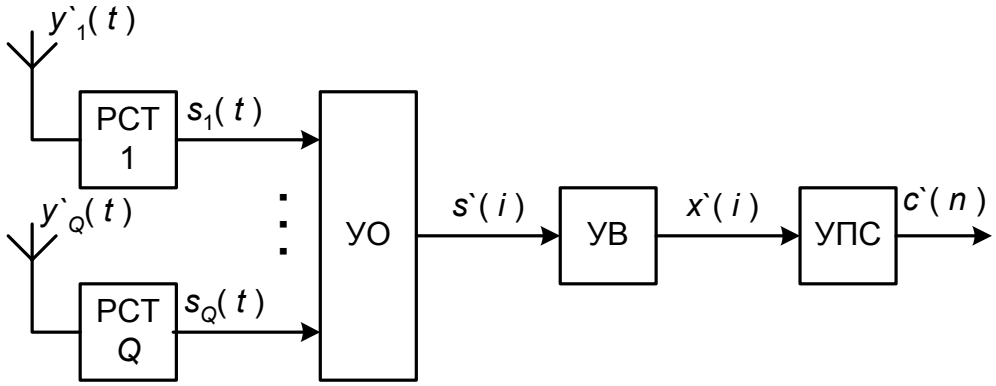

Рисунок 1 – Объединение сигналов на физическом уровне. Вариант 1

При частотно разнесенной передаче одних и тех же данных используются различные несущие радиочастоты, следовательно, параметры используемых каналов могут отличаться более значительно, чем в режиме пространственно разнесенного приема на одной радионесущей, в частности, величиной задержки и рассинхронизацией несущих частот. Поэтому прежде чем объединить сигналы предлагается в каждом канале предварительно выполнить процедуру восстановления формы сигнала. При этом будет обеспечено выравнивание временных задержек сигналов, прошедших по разным каналам, и формирование сигналов, близких или даже одинаковых по форме. На рисунке 2 изображена структурная схема, отображающая данный вариант объединения принимаемой информации при разнесенном приеме.

Предлагаемый способ объединения сигналов УПС реализуется следующим образом. Сначала принятый сигнал $s_q(t)$ обрабатывается в устройстве восстановления

$$x`_q(i) = \boldsymbol{s}_{\boldsymbol{q}}(i) * \boldsymbol{h}_{\mathbf{ув}}(i, \Delta f). \quad (7)$$

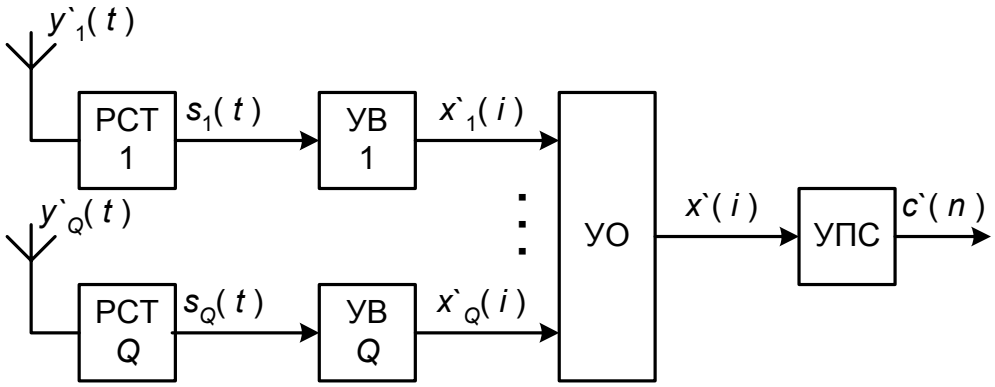

Рисунок 2 – Объединение сигналов на физическом уровне. Вариант 2

Обработанные сигналы $x`_q(i)$ поступают в устройство объединения физического уровня, в котором выполняется операция арифметического суммирования взвешенных отсчетов сигнала посылки

$$x`(i) = \sum_{q=1}^{Q} x`_q(i). \quad (8)$$

Далее над суммарным сигналом $x`(i)$ выполняются стандартные процедуры, аналогичные (1)...(3)

$$c`_{\text{ф}}(n) = \begin{cases} 0, & \textit{если} \quad R(n) < 0 \\ 1, & \textit{если} \quad R(n) \geq 0 \end{cases}, \quad (9)$$

$$b`_{\text{ф}}(m) = \Psi(\boldsymbol{c}`_{\boldsymbol{\text{ф}}}(m)), \quad (10)$$

$$\mu_{\text{ф}}(m) = \begin{cases} 0, & \textit{если} \quad \boldsymbol{S}(m) = 0 \\ 1, & \textit{если} \quad \boldsymbol{S}(m) \neq 0 \end{cases}. \quad (11)$$

Для проверки работоспособности предложенного способа были проведены статистические исследования путем моделирования на ЭВМ. На рисунке 3 приведена зависимость вероятности ошибки $P_{\text{ош}}$ от числа каналов разнесенного приема Q при воздействии импульсных помех на фоне гауссовского шума. Импульсные помехи имеют параметры: отношение амплитуды помехи к уровню информационного сигнала $A = 10…15$; длительность помехи $\tau = 100…400$ мс;

интервал между появлением помех $I = 10…12$ посылок. На рисунке 3 кривая 1 соответствует первому варианту объединения, кривая 2 – второму. Кривые получены для скорости передачи данных $c = 600$ бит/с при отношении уровня информационного сигнала к уровню гауссовского шума $h = 2$ во всех каналах разнесения.

Как видно, объединение сигналов по второму варианту обеспечивает лучшую помехозащищенность, чем по первому варианту.

На рисунке 4 приведена зависимость вероятности ошибки $P_{ош}$ от отношения сигнал/шум в каналах связи h при разном числе каналов разнесенного приема Q. Кривые 2 и 4 соответствуют объединению на канальном уровне, кривые 3 и 5 – на физическом уровне. Кривая 1 соответствует числу каналов разнесения $Q = 1$, кривые 2 и 3 – для $Q = 3$, кривые 4 и 5 – для $Q = 5$. Результаты получены для скорости передачи данных $c = 600$ бит/с.

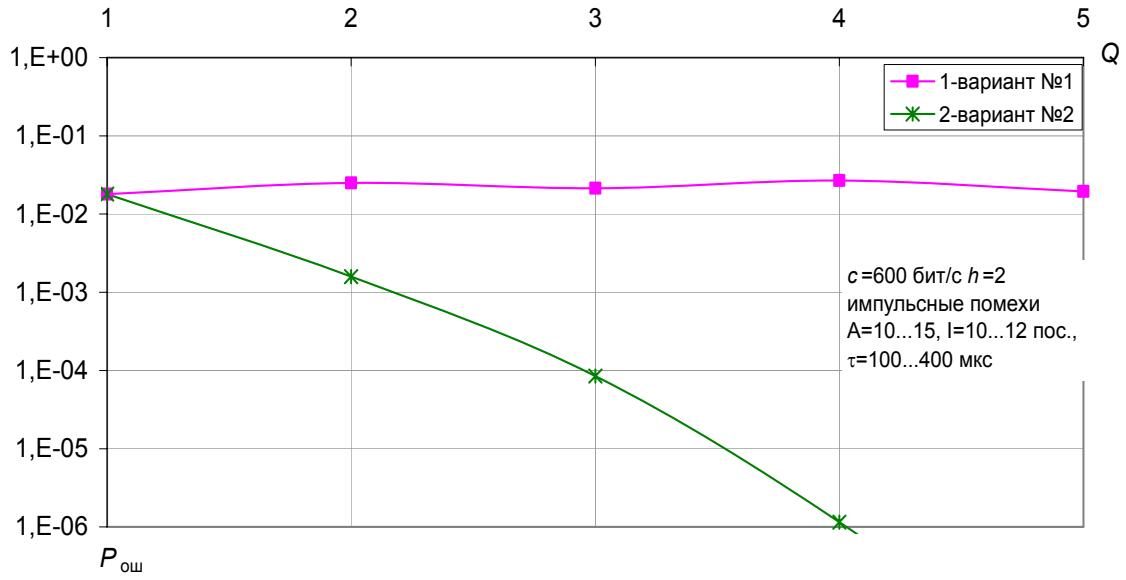

Рисунок 3 – Вероятность ошибки при двух вариантах объединения на физическом уровне

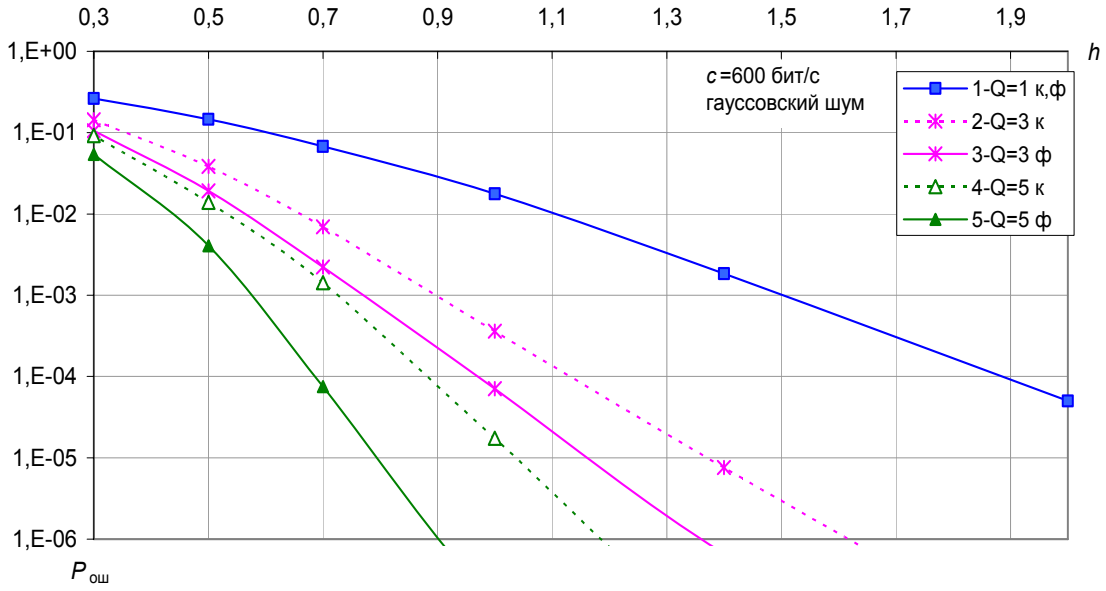

Рисунок 4 – Вероятность ошибки при объединении на физическом и канальном уровнях при воздействии гауссовского шума

На рисунке 5 приведена зависимость вероятности ошибки $P_{ош}$ от числа каналов разнесенного приема Q при воздействии импульсных помех на фоне гауссовского шума. Гистограмма 1 соответствует объединению на канальном уровне, гистограмма 2 – на физическом уровне. Результаты получены для скорости передачи данных $c = 600$ бит/с при отношении $h = 1$ во всех каналах разнесения и при тех же значениях параметров импульсных помех, что использовались при получении результатов, приведенных на рисунке 3.

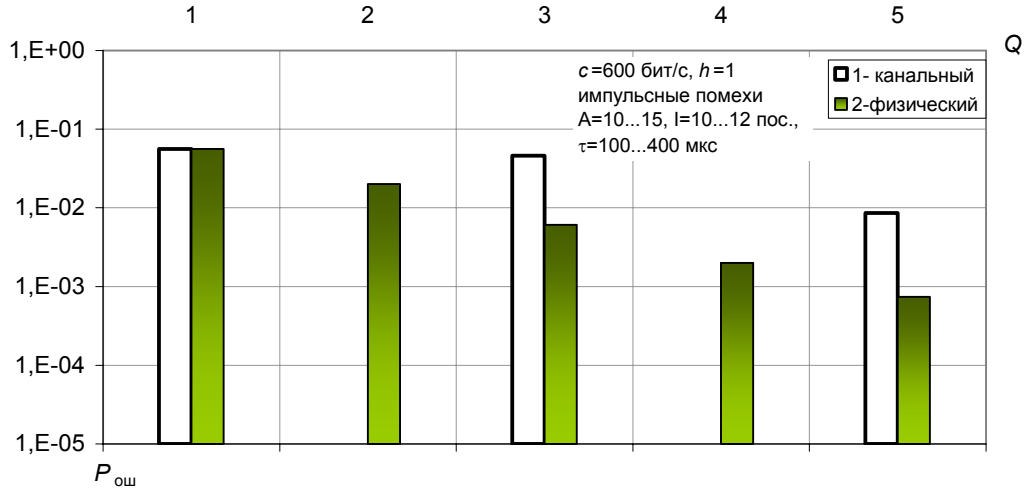

Рисунок 5 – Вероятность ошибки при объединении на физическом и канальном уровнях при воздействии импульсных помех на фоне гауссовского шума

Как видно из рисунков 4 и 5, объединение сигналов посылок на физическом уровне обеспечивает лучшую помехозащищенность, чем объединение битов на канальном уровне.

Использование процедуры объединения сигналов на физическом уровне в дополнение к процедуре объединения битов на канальном уровне расширяет функциональные возможности метода разнесенного приема, так как объединение информации может выполняться не только при нечетном числе каналов, но и при четном числе.

По результатам проведенных исследований можно сделать вывод, что предложенный способ объединения сигналов на физическом уровне при разнесенном приеме по второму варианту повышает доступность и целостность данных.

ЛИТЕРАТУРА:

1. Хмельницкий Э.А. Разнесенный прием и оценка его эффективности. М.: Связьиздат, 1960.
2. Злотник Б.М. Помехоустойчивые коды в системах связи. – М.: Радио и связь, 1989. – 232 с.
3. Кашаев Е.Д., Егорова Н.А. Модель защиты сигналов на физическом уровне автоматизированных систем. Вооружение, безопасность, конверсия: Материалы конференции 17-19 октября 2003 г. Ч. II. – Пенза: Изд-во Пенз. гос. ун-та, 2004. С. 111–119.
4. Кашаев Е.Д. Объединение сигналов при разнесенном приеме // Материалы VII Международной НПК «Информационная безопасность» – Таганрог: Изд-во ТРТУ, 2005. С.168–169.

Получено 19.12.2005. Опубликовано в Internet 20.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.24-27. Секция-8: Конфиденциальность, целостность, доступность
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/008)

ПОВЫШЕНИЕ СКОРОСТИ АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147 ЗА СЧЕТ ПРЕДВЫЧИСЛЕНИЙ

Коробов В.В., Грунтович М.М. E-mail: kbv@crystall.tl.ru
Пензенский государственный университет, ООО НПФ «Кристалл»

В реальном мире к программным реализациям криптографических алгоритмов помимо требований к достоверности отражения алгоритма на машинный код предъявляются еще и требования к скоростным характеристикам. Часто, если следовать точному описанию алгоритма, не удается достичь желаемой эффективности. Для повышения скоростных характеристик используются различные способы: распараллеливание выполнения шагов за счет внутренних возможностей аппаратной платформы, предварительные вычисления и т.д.

Рассмотрим способ, основанный на предварительном вычислении результатов выполнения некоторых шагов алгоритма. Суть его заключается в том, что до непосредственной программной реализации алгоритм подвергается анализу с целью определения шагов алгоритмов, выполнение которых можно заменить выборкой из массива заранее заготовленных результатов. Выигрыш заключается в более высокой скорости выборки из памяти по сравнению со скоростью прямого вычисления значений нескольких шагов алгоритма. При этом не стоит забывать о доступных машинных ресурсах, преодоление разумного порога которых сводит на нет все попытки оптимизации криптографического алгоритма. Ниже мы столкнемся с такой ситуацией.

Схема работы типового шага алгоритма шифрования по ГОСТ 28147 [1] приведена на рисунке 1.

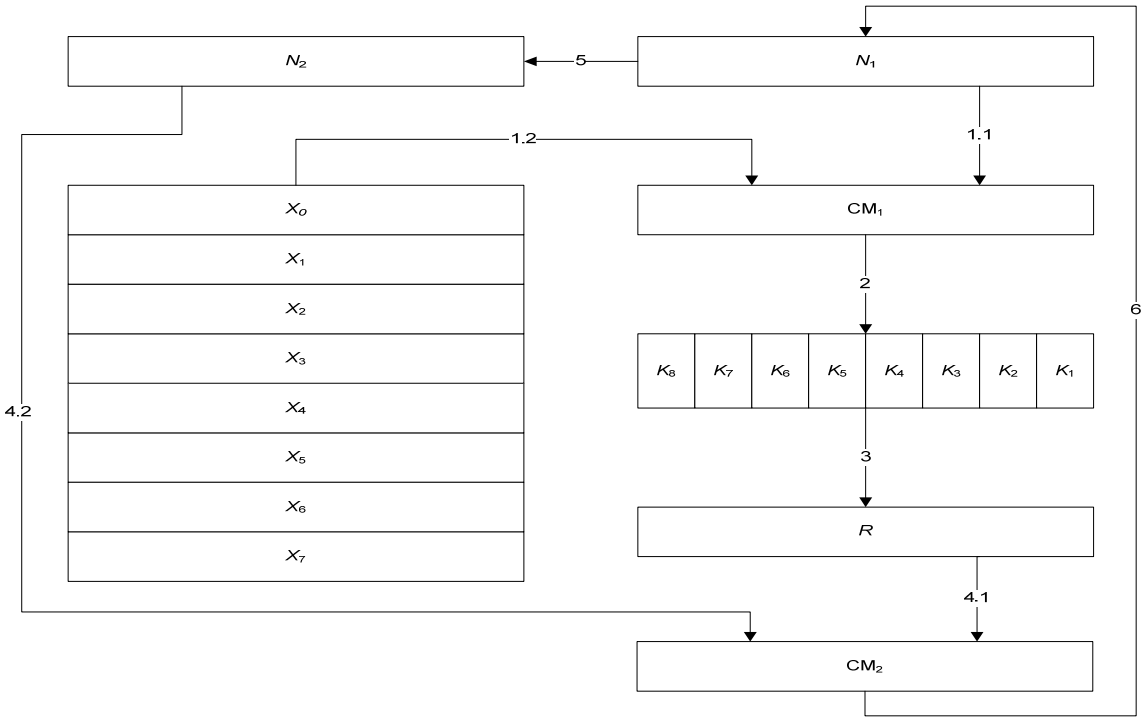

Рисунок 1 – Схема основного шага алгоритма шифрования ГОСТ 28147

Все накопители схемы, изображенной на рисунке 1, 32–разрядные. Накопители *N*1 и *N*2 содержат блоки открытого или шифрованного текста, в зависимости от реализуемого алгоритма шифрования или расшифрования. Накопители X_0, X_1, X_2, X_3, X_4, X_5, X_6 и X_7 образуют КЗУ, в котором содержится 256–битный ключ шифрования. Сумматоры $СМ_1$ и $СМ_2$ выполняют суммирование двух 32–битных блоков по модулю 2^{32} и 2 соответственно. Четырехбитные узлы замены K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8 образуют блок подстановки *K* (рисунок 2). Поступающий на вход блока подстановки 32–разрядный вектор разбивается на восемь последовательно идущих 4–разрядных векторов, каждый из которых преобразуется в 4–разрядный вектор соответствующим узлом замены K_i, представляющим собой таблицу из шестнадцати строк, содержащих по четыре бита заполнения в строке. Входной вектор определяет адрес строки в таблице, заполнение данной строки является выходным вектором. Затем 4–разрядные векторы последовательно объединяются в 32–разрядный. Регистр сдвига *R* осуществляет циклический сдвиг содержиморго на 11 разрядов влево.

4-битная каноническая реализация

При канонической реализации в соответствии с ГОСТ 28147 необходимо реализовать 8 подстановок битов 4×4 (см. рисунок 2).

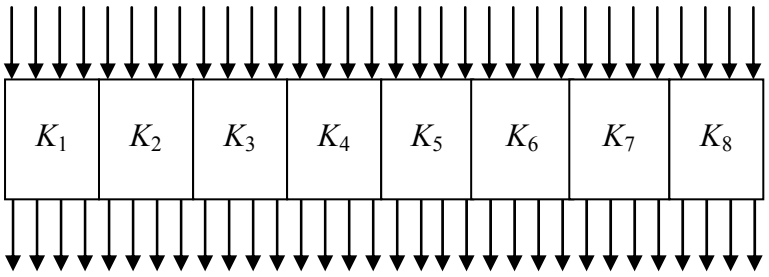

Рисунок 2 – Блок подстановок *K*

Каждая строка таблицы Ki занимает минимум 1 байт, поэтому такой подход потребует 8*24 = 128 байтов для хранения таблицы.

Однако, поскольку далее необходима установка 4-битного результата выборки в 32-битный регистр *R*, предлагается хранить таблицы замены в виде массива 32-битных векторов, учитывающих позицию результата замены в регистре *R*. Это тем более верно, учитывая то, что шины современных процессоров, как правило, 32-битные и оптимизированы для выполнения операций над такими единицами данных. Кроме того, при выполнении предвычислений на этапе подготовки таблиц замены можно выполнить последующий циклический сдвиг строк таблицы на 11 разрядов, ускорив тем самым работу алгоритма еще на одну операцию.

Итого хранение всех таблиц замены требуется 512 байтов памяти.

При этом выполнение операции подстановки *K* займет время, равное 8 циклам, каждый из которых состоит из:

- выделения 4-битного адреса из 32-битного входного вектора,
- выборки из памяти соответствующей таблицы замены 32-битной строки по адресу, определяемому этим вектором,
- накопление (исключающее «или») результата в регистре R.

8-битная традиционная оптимизация

Рассмотрим оптимизацию схемы, основанную на увеличении разрядности узлов замены, т.е. на попарном склеивании соседних подстановок K_i в подстановки 8×8 (рисунок 3). Назовем такую оптимизацию 8-битной или традиционной, поскольку она чаще всего используется при реализациях схемы шифрования ГОСТ 28147 (см., например, [2] и [3]).

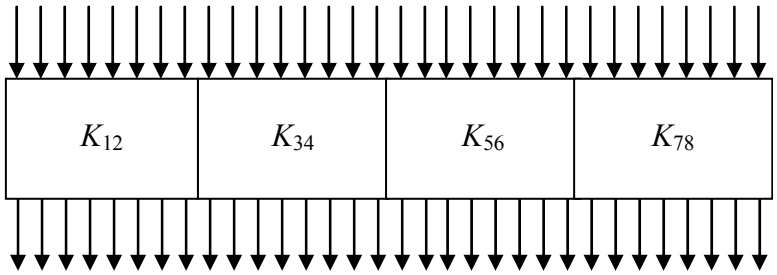

Рисунок 3 – Схема 8-битная оптимизация блока подстановок

При этом потребуется для хранения таблиц замены память для $4*2^8$ строк. При хранении каждой 8-битной строки результата в 32-битной ячейке (см. выше) получаем 4Кб памяти.

При этом каждый шаг подстановки требует выполнения 4 циклов команд:

- выделения 8-битного адреса из 32-битного входного вектора,
- выборки из памяти соответствующей таблицы замены 32-битной строки по адресу, определяемому этим вектором,
- накопление (исключающее «или») результата в регистре R.

Как видим, скорость на первый взгляд выросла в 2 раза, поскольку циклы для 4-битной и 8-битной реализации по существу не отличаются.

12-, 16- и 32-битные оптимизации

Продолжаем укрупнение таблиц замены за счет склеивания соседних перестановок K_i. Если склеить 3 соседних подстановки, получится 12-битная оптимизация. Она будет состоять из двух таблиц замены 12×12 и одной 8×8. Объединение четырех K_i приведет к 16-битной оптимизации, состоящей из двух таблиц замены 16×16. И, наконец, вырожденный случай: одна таблица замены 32×32. Причем цикл обработки состоит лишь из операции формирования адреса и выборки из памяти.

В таблице 1 приведены параметры эффективности различных типов реализаций – объем требуемой памяти и количество циклов команд, требуемых для реализации.

Таблица 1 – Эффективность вариантов оптимизации блока подстановок

Тип оптимизации	Размер таблицы замен, Кб	Количество циклов
4	0.5	8
8	4	4
12	33	3
16	512	2
32	16777216 (16Гб)	Меньше 1

В идеале наиболее скоростной выглядит 32-битная реализация, однако требуемый объем таблицы значений нереален. Мало того, уже 16-битная оптимизация с таблицей, допустимой по объему для современных компьютеров, проигрывает 8- и 12-битным реализациям. Причина в том, что обращение к полумегабайтному массиву постоянно приводит к подкачке с диска страниц

виртуальной памяти, что не только нивелирует выигрыш в скорости, но даже существенно замедляет работу. В операционной системе DOS виртуальная память не используется, но там выделение 512 Кб массива неконструктивно.

Как видно наиболее эффективно на практике использование 8– и 12–битной оптимизации ввиду приемлемого размера таблицы замен и наиболее высокой скорости работы. При этом при работе в DOS 12-битная оптимизация дает наивысшую скорость, в то время как в ОС Windows она иногда проигрывает 8-битной. Причина в многопоточности и, как следствие, в промахах кэша процессора при обращении к массиву такого размера.

ЛИТЕРАТУРА:

1. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

Получено 19.12.2005. Опубликовано в Internet 20.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.28-31. Секция-9: Аутентификация: парольная, биометрическая, криптографическая
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/009)

ФОРМАЛЬНЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ: МЕТОДЫ, ОСНОВАННЫЕ НА МОДЕЛЯХ КОНЕЧНЫХ АВТОМАТОВ

Давыдов А.Н.
НПФ «Кристалл»

Введение

Криптографический протокол обеспечивает достижение определённых целей безопасности. Однако если протокол содержит ошибки, то он может не достичь или достичь не в полной мере всех поставленных перед ним целей. Ошибки в протоколе могут быть неявными и трудно обнаруживаемыми. Существует множество примеров, когда ошибки обнаруживались в уже хорошо изученных протоколах. Ошибка, обнаруженная Деннинг и Сакко [1], в протоколе распределения ключей Нидхема и Шрёдера [2], позволяет злоумышленнику выдавать старый, скомпрометированный сеансовый ключ за новый. Протокол аутентификации МККТТ X.509, описанный в проекте стандарта [3], содержит ошибку, которая позволяет злоумышленнику выдавать старый сеансовый ключ за новый [4]. Формальные методы предназначены для решения этой проблемы. С одной стороны, они достаточно содержательны и позволяют легко выполнять моделирование и анализ протоколов; с другой стороны, они достаточно сложны и позволяют обнаруживать сложные для понимания ошибки, не выявленные при неформальном анализе.

Формальные методы на протяжении длительного времени использовались для анализа коммуникационных протоколов. Некоторые работы по анализу криптографических протоколов велись в конце семидесятых и в начале восьмидесятых годов [5], [6], [7]. Но в целом, применение формальных методов к криптографическим протоколам не было широко распространено до начала девяностых, когда при использовании методов формального анализа были найдены необнаруженные ранее ошибки в криптографических протоколах.

В настоящее время существуют следующие подходы применения формального анализа к криптографическим протоколам[1)]:

- методы, основанные на моделях конечных автоматов;
- использование логик знания и доверия;
- использование алгебр для моделирования состояния знаний субъектов о словах, используемых в протоколе.

Модель злоумышленника Долева-Яо

Большинство методов, основанных на конечных автоматах, используют модель злоумышленника, предложенную Долевым и Яо [5], [6]. В модели Долева-Яо все активные участники протокола разделяются на два вида: честные

[1)] Некоторые специалисты в области формального анализа [8] подразделяют подход, основанный на моделях конечных автоматов, на методы, использующие специально разработанные экспертные системы для разработки и исследования сценариев протокола, и методы, использующие языки описания и средства проверки, разработанные не специально для анализа криптографических протоколов.

участники (*honest participant*) и злоумышленник (*adversary*). Честные участники выполняют шаги протокола без отклонений. Они могут одновременно выполнять несколько сеансов протокола с различными участниками. Модель содержит сообщения, которыми обмениваются участники протокола, но не описывает внутренние состояния участников.

В модели Долева и Яо делается предположение, что среда передачи контролируется злоумышленником, который может читать весь трафик, изменять и удалять сообщения, создавать новые сообщения и выполнять любые операции, которые могут выполнять легитимные пользователи системы. Предполагается, что изначально злоумышленник не знает никакой секретной информации, например секретных ключей, принадлежащих легитимным пользователям системы.

Поскольку злоумышленник может удалять сообщения из канала связи и помещать в канал связи созданные им сообщения, то можно рассмотреть любое сообщение, посланное легитимным пользователем, как сообщение, посланное злоумышленнику, и любое сообщение, полученное легитимным пользователем, как сообщение, полученное от злоумышленника. Таким образом, система становится автоматом, используемым злоумышленником для генерации слов. Эти слова подчиняются определенным правилам подстановки, например таким, что шифрование и расшифрование на одном ключе отменяют друг друга. Таким образом, злоумышленник управляет системой с подстановкой элементов. Если цель злоумышленника состоит в том, чтобы узнать секретное слово, то проблема доказательства безопасности протокола становится проблемой определения слова в системе с подстановкой элементов. Долев и Яо, используя последний вывод, создали несколько алгоритмов для анализа ограниченного множества протоколов.

Модель Долева и Яо слишком ограничена и не подходит для анализа многих протоколов. Она может использоваться только для обнаружения ошибок, которые могут привести к нарушению конфиденциальности. Большинство методов анализа протоколов, использующих модель злоумышленника Долева и Яо, расширяют её, чтобы описать поведение участников протокола.

Экспертная система *Interrogator*

Одной из самых первых систем, использующих подход Долева и Яо, является *Interrogator* (Следователь), разработанный Милленом [9], [10]. *Interrogator* – это программное средство, разработанное на языке *Prolog*, которое пытается обнаруживать ошибки безопасности в протоколе путём полного перебора состояний протокола. Состояние протокола определяется совокупностью состояний всех его участников. Переходы между состояниями протокола происходят при передаче и/или приёме сообщений между его участниками. Сообщения участников перехватываются злоумышленником, который может удалять сообщения, создавать новые сообщения по известным ему сообщениям или пропускать сообщения без внесения изменений. Зная конечное состояние, в котором злоумышленник получает секретное слово, *Interrogator* будет подбирать все возможные пути достижения этого состояния. Если *Interrogator* находит такой путь, то он определяет его как ошибку безопасности.

Злоумышленник в *Interrogator* описывается выражением $p\_knows(x, H, q)$ где x – блок данных, известный злоумышленнику, H – множество накопленных злоумышленником сообщений, которые приводят к раскрытию x, q – состояние сети, достижимое из начального состояния. *p_knows* определяется как $p\_knows(x, H, q)$, если верно хотя бы одно из следующих выражений:

– x известен первоначально;

– ($H = H'sent(m)$ и $sent(m) : q' \rightarrow q$ и $H' : q_0 \rightarrow q'$ и $p\_gets(x, m, H', q')$);

– ($H = H'e$ and $e : q' \rightarrow q$ and $p\_knows(x, H', q')$);

– ($H' : q_0 \rightarrow q'$ and $p\_modifies(q', q, H)$ and $p\_knows(x, H', q')$).

Определение *p_knows* описывает способы, которыми злоумышленник, имея множество накопленных сообщений H, может узнать x в состоянии q. Злоумышленник может узнать x из последнего прочитанного нешифрованного сообщения m, может узнать x из предыдущего состояния q' (если в состоянии q' он знал x ($p\_knows(x, H', q')$)) или может узнать x, используя выражение *p_modifies*. Утверждение $p\_modifies(q', q, H)$ означает, что, если злоумышленник знает x в состоянии q', которое достижимо при множестве накопленных сообщений H, и нарушитель изменяет сообщение таким образом, что криптографическая система переходит в состояние q, которое достижимо при множестве накопленных сообщений H, то злоумышленник продолжает знать x.

Аналогично, *p_gets* определяется как $p\_gets(x, m, H, q)$, если верно хотя бы одно из следующих выражений:

– x является частью m;

– ($\{m'\}_k$ является частью m and $p\_knows(k, H, q)$ and $p\_gets(x, m', H', q)$).

Определение *p_gets* устанавливает, что злоумышленник может читать любое сообщение, но если сообщение зашифровано, то он может его извлечь, только если знает ключ шифрования.

Поскольку в *Interrogator* реализован метод полного перебора состояний, то он требует значительных временных ресурсов для анализа протокола. Кроме того, возможно незавершение выполнения анализа в силу специфики методов поиска, реализованных в языке *Prolog*. *Interrogator* не нашёл ранее неизвестных атак на криптографические протоколы, но смог распознать множество известных атак [10].

Экспертная система Лонглейя-Ригби

Другие системы анализа используют механизмы, реализованные в *Interrogator*, но допускают человеческое вмешательство в процессе поиска. Например, система поиска, разработанная Лонглейем и Ригби [11] используется для поиска неявных и ранее неизвестных ошибок в иерархических системах управления ключами. Главное различие между системой Лонглейя-Ригби и *Interrogator* заключается в том, что средство Лонглейя-Ригби допускает человеческое вмешательство. Каждый раз, когда система полагает, что слово не может быть найдено злоумышленником, оператор может вмешаться и установить, так ли это на самом деле. Если делается вывод, что слово является достижимым, то эту информацию можно внести в базу данных и продолжить поиск.

Метод формальной проверки Кеммерера

Новым витком развития методов, основанных на конечных автоматах, стало моделирование Кеммерером криптографических протоколов на непроцедурном языке формального описания *Ina Jo* [10]. Язык *Ina Jo* был разработан и до этого всегда использовался для доказательства правильности программного обеспечения. Кеммерер показал, как можно смоделировать на этом языке атаки на протоколы, и использовал пошаговое описание, чтобы «пройти» несколько смоделированных атак. Как и Миллен, Кеммерер моделирует криптографические протоколы как сообщающиеся конечные автоматы. Так как протоколы смоделированы на языке описания, к которому присоединено средство для доказательства теорем, то можно использовать данное средство для

доказательства теорем о безопасности протоколов, определяя свойства безопасности как инвариантные состояния и доказывая, что эти состояния остаются инвариантными после каждого перехода.

В качестве примера Кеммерер рассматривает распределённую криптографическую систему, состоящую из сервера аутентификации и терминалов, и находит в ней недостатки. Практическая полезность метода Кеммерера ограничена в силу того, что он пытается доказать корректность, а не безопасность протокола. Кроме того, разработанная модель содержит шаблоны только известных атак.

Выводы

Возможности всех методов анализа, основанных на моделях конечных автоматов, ограничены. Они позволяют находить только известные недостатки в криптографических протоколах. Системы, в которых реализованы идеи данного подхода, как правило, имеют низкую эффективность, поскольку поиск в них осуществляется методом полного перебора.

ЛИТЕРАТУРА:

1 D.E. Denning and G.M. Sacco. Timestamps in key distribution protocols. Communications of the ACM, 24(8): pages 533-536, August 1981.

2 R.M. Needham and M.D. Schroeder. Using Encryption for Authentication in Large Networks of Computers. Communications of the ACM, 21(12): pages 993-999, December 1978.

3 CCITT. CCITT Draft Recommendation X.509. The Directory-Authentication Framework, Version 7, November 1987.

4 M. Burrows, M. Abadi, and R. Needham. A logic of authentication. ACM Transactions on Computer Systems, 8(1): pages 18-36, February 1990.

5 D. Dolev and A. Yao. On the security of public key protocols. Communications of the ACM, 29: pages 198-208 August 1983.

6 D. Dolev, S. Even, and R. Karp. On the security of ping-pong protocols. Information and Control, pages 57-68 1982.

7 M.J. Merritt. Cryptographic Protocols. Ph.D. thesis, Georgia Institute of Technology, 1983.

8 A.D. Rubin and P. Honeyman. Formal methods for the analysis of authentication protocols. Draft manuscript, 1994.

9 J.K. Millen, S.C. Clark and S.B. Freedman. The interrogator: Protocol security analysis. IEEE Transactions on Software Engineering, SE-13(2), 1987.

10 R. Kemmerer, C. Meadows and J. Millen. Three systems for cryptographic protocol analysis. Journal of Cryptology, 7(2), 1994.

11 D. Longley and S. Rigby. An automatic search for security flaws in key management schemes. Computers and Security, 11(1): pages 75-90, 1992.

Получено 26.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.32-40. Секция-2: Информационная безопасность сложных систем
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/010)

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Сапегин Л.Н., Бочкарев С.Л. e-mail: bosl@crystall.tl.ru
ООО НПФ «Кристалл»

Введение

Важнейшее значение для обеспечения безопасности организаций в информационной сфере придается системам менеджмента информационной безопасности (СМИБ). Обобщенная математическая модель, позволяющая оценивать эффективность СМИБ, учитывающая экономические, временные, вероятностные и иные характеристики, представлена ниже. Предлагаемая модель может быть детализирована для конкретной организации или любой ее части, включая ИТ-системы, персонал, информацию, процессы деятельности и т.д.

Модель оценки эффективности системы менеджмента информационной безопасности

На основании материалов [1] разработана и представлена ниже математическая модель, позволяющая провести оценку эффективности СМИБ.

Пусть С = С(t) – стоимость ведения бизнеса организацией за время от нуля до t, Д = Д(t) - её доход к моменту t, П = П(t) – прибыль (всё в условных единицах стоимости: у. е.). Предполагается, что в отсутствии инцидентов функции С, Д и П являются линейными функциями времени, равными нулю при t = 0 и связанными зависимостью П(t) = Д(t) – С(t) (см. рисунок 1).

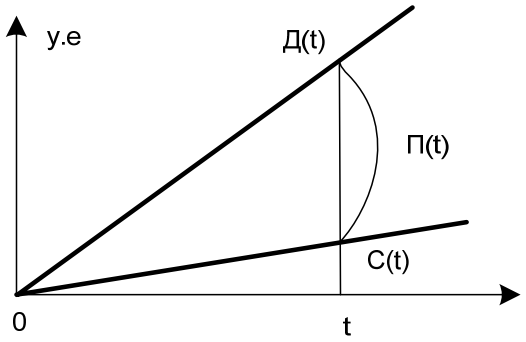

Рисунок 1 - Прибыль в отсутствии инцидента

При возникновении инцидента в момент Т и отсутствии реакции на него со стороны организации в течение временного «окна» ΔТ (зависящего от типа инцидента) данная организация терпит ущерб в размере У (у. е.) в момент Т + ΔТ и, возможно, снижается активность бизнеса (уменьшается угол наклона прямой Д(t) после момента времени Т + ΔТ) (см. рисунок 2).

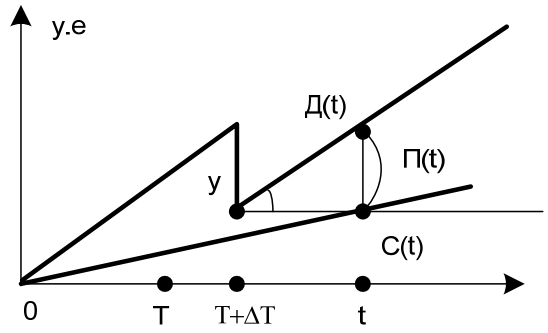

Рисунок 2 – Влияние инцидента

В худшем случае активность бизнеса может прекратиться и рост дохода может остановиться на уровне Д(Т + ΔТ) – У. В лучшем случае П(t) = Д(t) – У – С(t), т. е. доход, а следовательно, и прибыль уменьшаются на У (у. е.).

Для максимизации прибыли организация создаёт СМИБ, начальная стоимость создания которой равна $С_К$ (у.е.), и стоимость ведения бизнеса становится равной С(t) + $С_К$ без учёта текущих затрат на обработку инцидентов в процессе эксплуатации СМИБ.

Защитные меры (в составе СМИБ) должны обнаружить инцидент в момент Тоб > Т и остановить его действие к моменту $Т_{ст} > Т_{об}$, причём должно быть $Т_{ст}$ – Т ≤ ΔТ. В этом случае ущерба У не будет, но СМИБ затрачивает $С_{ст}$ (у. е.) на обработку инцидента, что снижает прибыль на величину $С_{ст}$, но сохраняет активность бизнеса (доход Д(t) после момента $Т_{ст}$ растёт с той же скоростью) (см. рисунок 3).

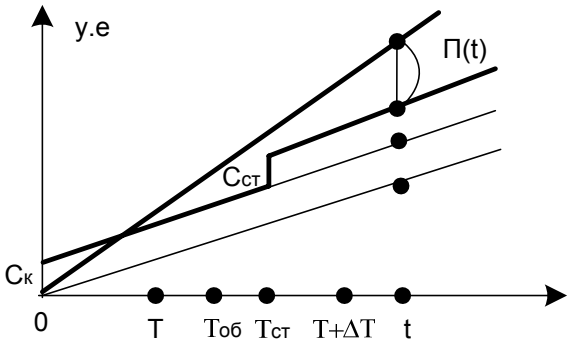

Рисунок 3 – Успешная обработка

Если же защитные меры СМИБ обнаруживают инцидент в момент $Т_{об} \geq Т + ΔТ$ или $Т_{об} < Т + ΔТ$, но $Т_{ст} > Т + ΔТ$, тогда в момент Т + ΔТ доход падает на величину У (у. е.), а в момент $Т_{ст}$ расход на обработку инцидента поднимается до величины $С'_{ст} \geq С_{ст}$ (см. рисунок 4).

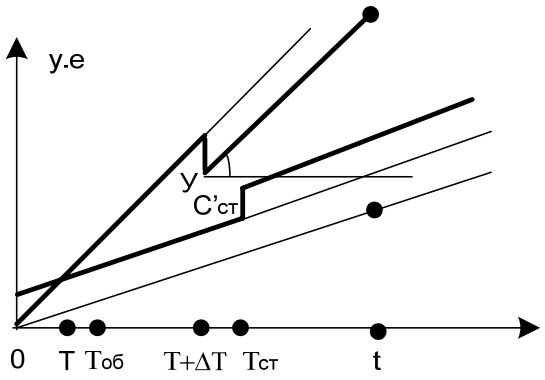

Рисунок 4 – Запоздалая обработка

В обоих случаях активность бизнеса может снижаться, а в случае обнаружения инцидента внешним источником (например, из сообщения от CERT) в момент $T_{вн} >> T + \Delta T$, активность бизнеса может прекратиться даже после обработки инцидента в момент $T_{ст} > T_{вн}$ (см. рисунок 5).

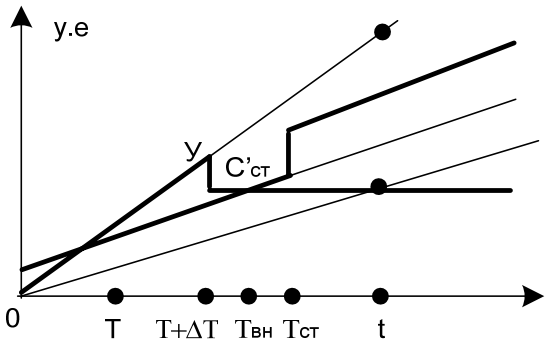

Рисунок 5 – Остановка бизнеса

Примечание: Все времена, в принципе, могут быть измерены непосредственно с некоторой точностью, позволяющей классифицировать защитные меры СМИБ по эффективности.

Классы эффективности защитных мер СМИБ

Защитные меры СМИБ можно подразделить на семь классов эффективности.

Класс 1. Тип: превентивные меры, которые позволяют предотвратить появление инцидента или мгновенно его обнаружить и предотвратить ущерб (времена $T_{об} – T$ и $T_{ст} – T_{об}$ очень малы).

Класс 2. Тип: обнаруживающие меры, которые позволяют обнаружить инцидент и реагировать достаточно быстро, чтобы успеть обработать его в пределах «окна» ΔT без существенных затрат и ущерба (время $T_{об}–T$ достаточно мало, чтобы $T_{ст} < T+\Delta T$).

Класс 3. Тип: обнаруживающие меры, которые позволяют обнаружить инцидент и на пределе успеть обработать его в пределах «окна» ΔT с существенными затратами, но без ущерба (время $T_{об} – T$ довольно велико, но всё же $T_{ст} \leq T + \Delta T$).

Класс 4. Тип: обнаруживающие меры, которые позволяют обнаружить инцидент, но не позволяют успеть обработать его в пределах «окна» ΔT (время $T_{об} - T$ так велико, что $T_{ст} > T + \Delta T$).

Класс 5. Тип: пассивные меры, которые не позволяют обнаружить инциденты, но имеют частично применяемый план непрерывности бизнеса, запускаемый в момент $T_{вн}$ (момент времени $T_{вн} >> T + \Delta T$; время $T_{ст} - T_{вн}$ достаточно мало).

Класс 6. Тип: пассивные меры, которые не позволяют обнаружить инциденты, но имеют некоторый план непрерывности бизнеса (момент времени $T_{вн} >> T + \Delta T$; время $T_{ст} - T_{вн}$ довольно велико).

Класс 7. Тип: пассивные меры, которые не позволяют обнаружить инциденты и не имеют какого-либо плана непрерывности бизнеса; в момент времени $T_{вн}$ данные меры позволяют начинать действовать по «обстановке» (момент времени $T_{вн} >> T + \Delta T$; время $T_{ст} - T_{вн}$ очень велико).

Категории эффективности СМИБ

СМИБ можно подразделить на семь категорий эффективности:

- наименее эффективная;
- гораздо ниже средней эффективности;
- ниже средней эффективности;
- средней эффективности;
- выше средней эффективности;
- гораздо выше средней эффективности;
- наиболее эффективная.

Наименее эффективная СМИБ:

- отказ любой защитной меры (средства) либо не обнаруживается, либо обнаруживается, но слишком поздно;
- обнаруживающие защитные меры либо не позволяют обнаруживать инциденты, либо позволяют обнаруживать их слишком поздно;
- нет никакого плана непрерывности бизнеса; любой инцидент - всегда полная неожиданность для СМИБ.

Наиболее эффективная СМИБ:

- любой отказ любой защитной меры (средства) обнаруживается немедленно и восстанавливается в пределах «окна» ΔT;
- все обнаруживающие защитные меры (средства) имеют класс 2 и выше;
- план непрерывности бизнеса разработан настолько подробно, что любой инцидент полностью обрабатывается в пределах «окна» ΔT.

Из сравнения этих крайних случаев выделяются 3 основные свойства эффективности СМИБ:

- *А. Способность обнаруживать отказы самих защитных мер (средств) СМИБ*;
- *Б. Способность обнаруживать и быстро реагировать на инциденты*;
- *В. Способность противодействовать инцидентам в непредвиденных обстоятельствах*.

СМИБ может обладать свойствами *А, Б* и *В* в разной степени. По определению, СМИБ средней эффективности обладает свойствами *А, Б* и *В* в средней степени.

СМИБ средней эффективности:

– имеются защитные меры (средства), позволяющие обнаруживать отказы, как других защитных средств, так и свои собственные;

– имеются обнаруживающие защитные меры (средства) классов 2 и 3, которые могут деградировать до класса 4;

– имеются защитные меры (средства) класса 6 или 5, позволяющие противостоять некоторым видам аварий, катастроф и других чрезвычайных происшествий (например, пожарам). Остальные чрезвычайные происшествия преодолеваются действиями «по обстановке».

СМИБ с эффективностью ниже средней обладает одним из свойств ниже среднего.

СМИБ с эффективностью гораздо ниже средней обладает двумя свойствами ниже среднего.

СМИБ с эффективностью выше средней обладает одним из свойств выше среднего.

СМИБ с эффективностью гораздо выше средней обладает двумя свойствами выше среднего.

Наименее эффективная СМИБ имеет все три свойства ниже среднего.

Наиболее эффективная СМИБ имеет все три свойства выше среднего.

Предлагается следующая система начисления очков: за выполнение любого из свойств на среднем уровне даётся 3 очка, за превышение уровня +1 очко, за снижение –1 очко, за значительное превышение +2 очка, за значительное снижение –2 очка. Таким образом, СМИБ принадлежит категории:

- **гораздо выше средней**, если число очков ≥11;
- **выше средней**, если число очков 10;
- **средней**, если число очков 9;
- **ниже средней**, если число очков 6÷8;
- **гораздо ниже средней**, если число очков ≤4.

Условие стационарности процесса обслуживания инцидентов

Инцидент, возникший в момент времени T, обнаруживается в момент $T_{об} > T$ защитными мерами, которые заканчивают его обработку в момент $T_{ст} > T_{об}$. Разность $T_{ст} - T = \Delta T_{и}$ (ед. времени/инц) назовём *временем обслуживания инцидента*. Если инцидент не успевает обслужиться к моменту времени $T + \Delta T$, то в этот момент он наносит ущерб бизнесу; ΔT – задержка нанесения ущерба инцидентом. Условием предотвращения ущерба является неравенство: $\mathbf{\Delta T > \Delta T_{и}}$ (см. рисунок 6).

Предположим, что поток инцидентов имеет интенсивность λ (инц/ед. времени), равную среднему числу инцидентов в единицу времени. Тогда средняя длина интервала времени между соседними инцидентами равна λ^{-1} (ед. времени/инц). Из теории массового обслуживания [2] известно, что очередь инцидентов на обслуживание не будет неограниченно возрастать, если $\mathbf{\Delta T_{и} < \lambda^{-1}}$. В противном случае ($\Delta T_{и} \geq \lambda^{-1}$) очередь становится сколь угодно большой. Условием предотвращения ущерба и ограниченности очереди на обслуживание инцидентов является неравенство: $\mathbf{\Delta T_{и} < \Delta T < \lambda^{-1}}$ (см. рисунок 6).

В теории массового обслуживания условие стационарности $\Delta T_{и} < \lambda^{-1}$ строго доказывается в предположении, что поток инцидентов является рекуррентным, т. е. интервалы времени между соседними инцидентами являются независимыми случайными величинами с одинаковой функцией распределения $F(t) = P\{T' - T<t\}$ [2]. Если, в частности, $F(t) = 1 - e^{-\lambda t}$, т.е. поток пуассоновский, то

можно в явной форме вычислить вероятность $P_{\geq n}(\Delta T_и)$ появления не менее «n» инцидентов за время $\Delta T_и$ обслуживания одного инцидента.

$$P_{\geq n}(\Delta T_{\grave{e}}) = 1 - \sum_{k=0}^{n-1} (\lambda \cdot \Delta T_{\grave{e}})^k (k!)^{-1} e^{-\lambda \cdot \Delta T_{\grave{e}}},$$

где n = 1, 2, …

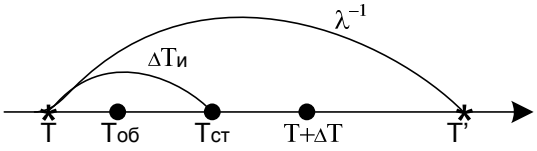

Рисунок 6 – Условие стационарности

Если же поток инцидентов не рекуррентный и интервалы времени между инцидентами «k» и «k+1» распределены по закону $F_k(t)$ с параметром $\lambda = \lambda_k$, где все λ_i при i = 1,2,… различны, то вероятности $P_{\geq n}(\Delta T_и)$ также можно вычислить в явной форме, например, по следующей приближённой формуле [3]:

$$P_{\geq n}\left(\Delta T_{\grave{e}}\right) \approx \left(\lambda_1 \cdot \lambda_2 \cdots \lambda_n\right) \cdot \left(n!\right)^{-1} \cdot \left(\Delta T_{\grave{e}}\right)^n,$$

где n = 1, 2, …

Последняя формула представляет интерес в случае зависимых (например, провоцирующих) инцидентов, когда появление первого инцидента (с интенсивностью λ_1) повышает вероятность появления второго (с интенсивностью $\lambda_2 > \lambda_1$), затем третьего (с интенсивностью $\lambda_3 > \lambda_2$) и т. д.

Лавинообразное нарастание ущерба от инцидентов происходит при условии:

$$\Delta T_{\grave{e}} \geq \Delta T \geq \lambda^{-1}.$$

Рентабельность СМИБ

Предположим, что защитные меры СМИБ работают циклами длины τ (ед. времени), причём в течение времени t они «включены» на обнаружение и обработку инцидентов, а в течение (τ–t) они «выключены»; ($0 \leq t \leq \tau$). Ожидается, что при фиксированном τ существует оптимальное значение t*: $0 \leq t^* \leq \tau$, при котором полные расходы R(t) на содержание СМИБ становятся минимальными, т.е. R(t*) = min R(t), где минимум берётся по t: $0 \leq t \leq \tau$.

Введём следующие обозначения:

- λ (инц/ед. времени) – интенсивность потока инцидентов;
- c (у.е./инц) – стоимость обработки одного инцидента;
- r (у.е./инц) – ущерб от одного инцидента;
- α (у.е./ед. времени) - стоимость применения обнаруживающих защитных мер (например, использования мониторинга) в течение выбранной единицы времени.

На отрезке [0; t] среднее число инцидентов равно λt, и средние расходы на обнаружение (мониторинг) и обработку инцидентов составят: (αt + λt·c) (у. е.). На отрезке [t; τ] среднее число инцидентов равно λ(τ – t) и средний ущерб при «выключенных» защитных мерах СМИБ составит: λ(τ – t)·r (у. е.) (см. рисунок 7). Полные средние расходы за 1 цикл составят:

$$R(t) = \alpha t + \lambda t \cdot c + \lambda(\tau - t) \cdot r$$

или

$$R(t) = (\alpha + \lambda c - \lambda r)t + \lambda \tau r .$$

Поскольку функция R(t) – линейная, то она принимает минимальное значение либо при t = 0, либо при t = τ (см. рисунок 8).

Если α + λc – λr < 0, т. е.

$$\alpha \cdot \lambda^{-1} < r - c, \qquad (1)$$

тогда min R(t) = R(τ) = α τ + λ τ c.

Если α + λc – λr > 0, т. е.

$$\alpha \cdot \lambda^{-1} > r - c, \qquad (2)$$

тогда min R(t) = R(τ) = λ τ r.

В условиях (1) и (2) величина $\boldsymbol{\lambda^{-1}}$ (ед. времени/инц) есть среднее время между инцидентами в потоке интенсивности **λ** (инц/ед. времени); $\boldsymbol{\alpha\ \lambda^{-1}}$ – средняя стоимость обнаружения (мониторинга) одного инцидента. Условие (1) означает, что риск r от одного инцидента должен превосходить стоимость обработки инцидента плюс стоимость (затраты) на обнаруживающие защитные меры (например, мониторинг) до возникновения очередного инцидента.

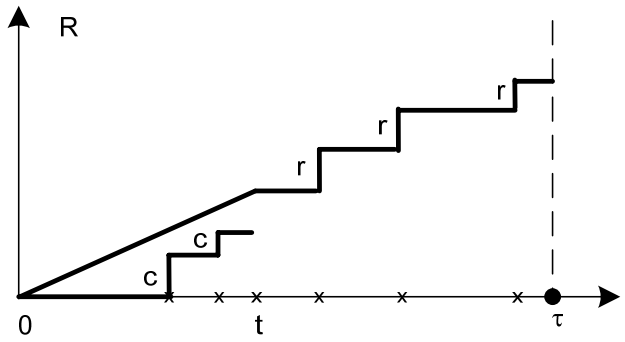

Рисунок 7 - Графики расходов на содержание СМИБ

Таким образом, защитные меры СМИБ должны быть «включены» в течение всего времени τ, пока выполняется условие (1). Защитные меры СМИБ должны быть «выключены», как только начнёт выполняться условие (2), например, по причине уменьшения интенсивности λ, в результате чего стоимость работы обнаруживающих защитных мер (например, мониторинга) превышает выигрыш **r – c**, получаемый от обработки риска.

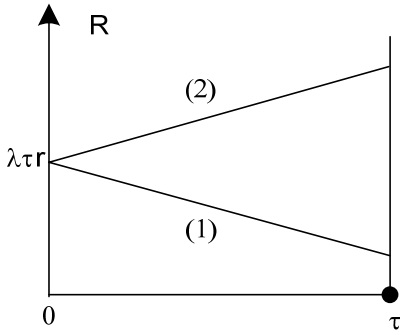

Рисунок 8 - Минимум функции R(t)

Условия (1) и (2) обобщаются на поток инцидентов, состоящий из инцидентов различных «k» типов. Если поток инцидентов типа «i» имеет интенсивность λ_i со стоимостью обработки c_i инцидентов с риском r_i , то:

$$R(t) = \alpha t + \sum_{i=1}^{k} \lambda_i \cdot t \cdot c_i + \sum_{i=1}^{k} \lambda_i \cdot (\tau - t) \cdot r_i$$

или

$$R(t) = \left(\alpha + \sum_{i=1}^{k} \lambda_i \cdot c_i - \sum_{i=1}^{k} \lambda_i \cdot r_i \right) \cdot t + \tau \cdot \sum_{i=1}^{k} \lambda_i \cdot r_i ,$$

откуда следуют условия:

$$\sum_{i=1}^{k} (\lambda_i / \lambda) \cdot (r_i - c_i) > \alpha \cdot \lambda^{-1} (1)';$$

$$\sum_{i=1}^{k} (\lambda_i / \lambda) \cdot (r_i - c_i) < \alpha \cdot \lambda^{-1} (2)';$$

$$\lambda = \lambda_1 + ... + \lambda_k .$$

Выводы

Вышеприведенные подходы, математическая модель оценки эффективности защитных мер СМИБ и предлагаемая система классификации защитных мер СМИБ могут быть использованы для оценки степени эффективности защитных мер, выбираемых для снижения оцененных рисков организации. Они позволяют учесть многие наиболее существенные факторы: экономические характеристики бизнес-деятельности организации, условия ведения ее бизнеса, в том числе, угрозы и уязвимости, реализуемые угрозы (инциденты), а также риски (возможные ущербы).

Модель позволяет динамически управлять эффективностью защитных мер с учетом изменчивости внутренней и внешней среды организации. Такая возможность управления «силой» защитных мер и затратами на их поддержание является одним из способов построения СМИБ, максимально эффективной с точки зрения достижения результата и затрат на ее разработку, внедрение и поддержание.

Такой подход к построению СМИБ является общепризнанным и наиболее перспективным. Он позволяет формировать адекватный рискам организации

бюджет службы безопасности, а также соответствующую информационную и организационно-техническую базу по обеспечению безопасности организации.

ЛИТЕРАТУРА:

1 D. Brever, W. List. «Measuring the effectiveness of an internal control system», Gamma Secure Systems Limited, 2004.
2 Б.В. Гнеденко, И.Н. Коваленко. Лекции по теории массового обслуживания, Киев, 1964.
3 Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьёв. Математические методы в теории надёжности. Изд. «Наука», Москва, 1965.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.41-45. Секция-2: Информационная безопасность сложных систем
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/011)

ОЦЕНКА ВЕРОЯТНОСТЕЙ СОСТОЯНИЙ ВЫХОДНЫХ РАЗРЯДОВ ПРЕОБРАЗОВАТЕЛЯ БИОМЕТРИЯ/КОД: МОДЕЛИРОВАНИЕ ЗАКОНА РАСПРЕДЕЛЕНИЯ

Иванов А.И., Надеев Д.Н.
Лаборатория биометрических и нейросетевых технологий
Пензенского научно-исследовательского электротехнического института

Сложность определения стойкости высоконадежных биометрических механизмов объясняется высокой размерностью используемых в них преобразователей, определяющей сопоставимость уровней стойкости биометрической и криптографической аутентификации. Перечень основных функциональных показателей контроля средств биометрическо-криптографической защиты регламентирован [1], при попытках оценки показателей контроля остро встает вопрос о корректном математическом описании выходных состояний нейросетевого преобразователя биометрия/код. Дать их единообразную форму математического описания трудно. Подходить к решению этой задачи разумно с простейшего случая биометрического средства с однослойной искусственной нейронной сетью. В простейших однослойных сетях, используемых в настоящий момент лабораторией ЛБНТ ФГУП «ПНИЭИ», используется 416 параметров, извлекаемых из оцифрованного биометрического образа (рисунок 1).

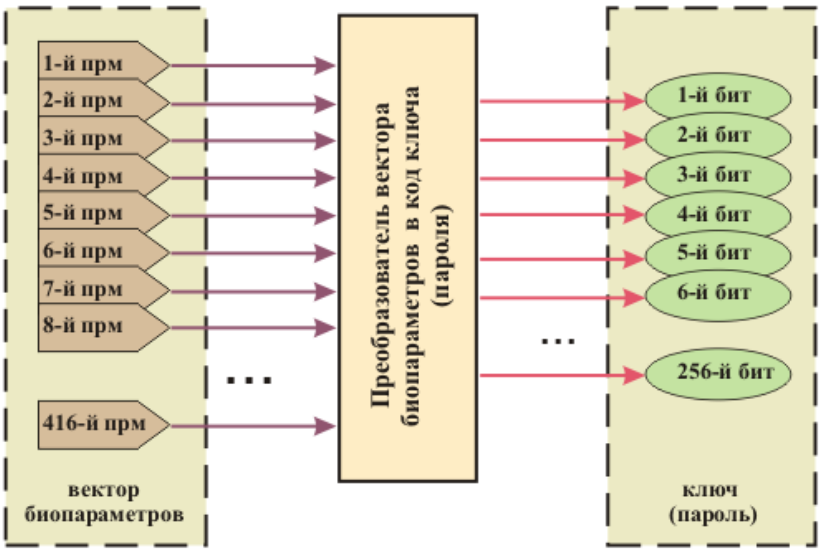

Рисунок 1 – Преобразование рукописного образа в код ключа аутентификации длинной 256 бит

Стандарт [1] определяет требования к процедуре обучения искусственной нейронной сети: используемые для этого образы «СВОЙ» подаются на вход преобразователя, на входе автомата обучения должен присутствовать ключ (пароль). После обучения при подаче образов «СВОЙ» на выходе должен получаться ключ, при подаче случайных биометрических образов «ЧУЖИЕ» – случайные состояния выходов. Эта ситуация отображена на рисунке 2. Заметим, что при подаче на входы обученной нейросети множества векторов «Свой»

выходные коды преобразователя должны повторяться, соответственно, корреляция между парой любых выходов нейросети будет близка к ±1. Напротив, при подаче на входы нейросети примеров векторов «Чужие» выходные коды должны быть случайны, то есть любая пара выходов нейросети должна иметь нулевую корреляцию.

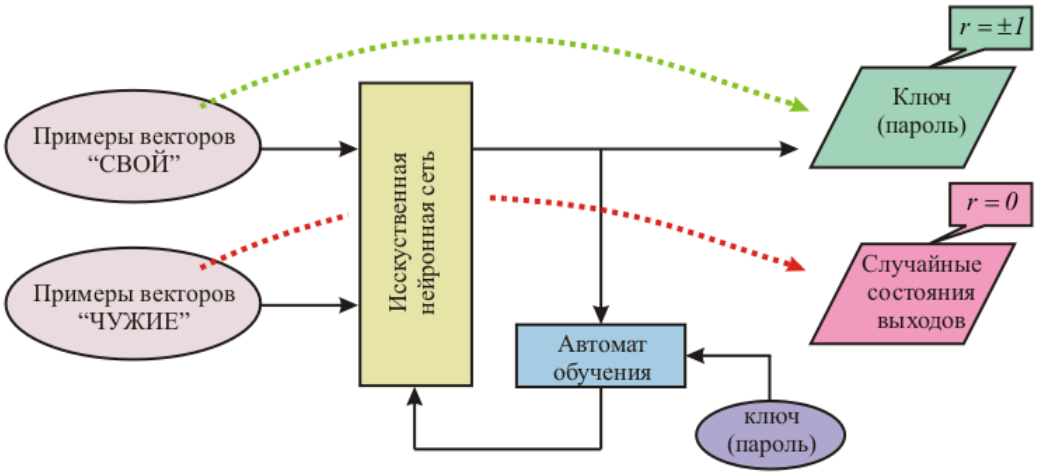

Рисунок 2 – Процедура обучения нейросетевого преобразователя векторов биометрических параметров в ключ (пароль)

Высоконадежное средство биометрической аутентификации должно гарантировать качество выходного «белого» шума при нейросетевой обработке случайных входных образов «Чужие». Каждый разряд выходного кода должен:

1) иметь близкие к равновероятным состояния «0» и «1»;
2) иметь нулевые коэффициенты парной и групповой корреляции.

В случае идеальной нулевой корреляции выходных данных искусственной нейросети преобразователя биометрия/код мера Хемминга отклонения выходного кода от заданного при обучении на образах «Свой» описывается биномиальным законом распределения значений.

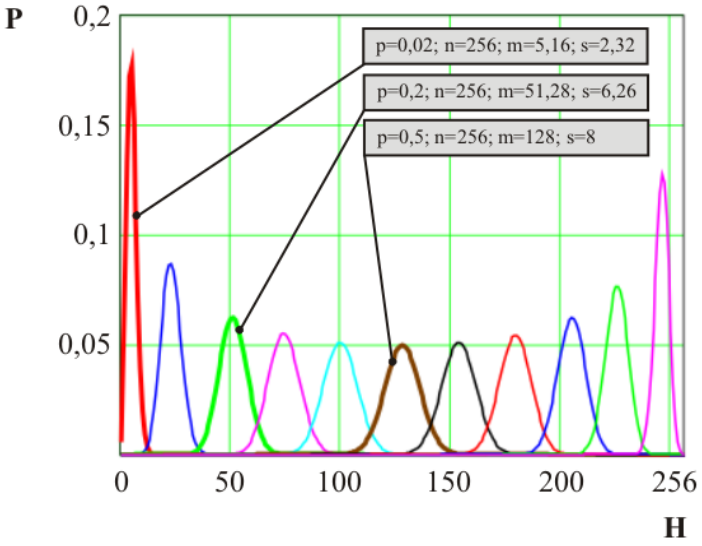

Рисунок 3 – Биномиальный закон распределения меры Хемминга (H) при независимых (некоррелированных) разрядах выходного кода

В простейшем случае независимых кодов с равной вероятностью состояний «0», «1» биномиальный закон трансформируется в нормальный. Эта ситуация условно отражена на рисунке 3. В случае увеличения корреляционной зависимости между выходными кодами нормальный закон постепенно трансформируется в равномерный, а затем в закон арксинуса. Эволюция гистограмм распределений меры Хемминга при входных биометрических данных разной коррелированности показана на рисунке 4.

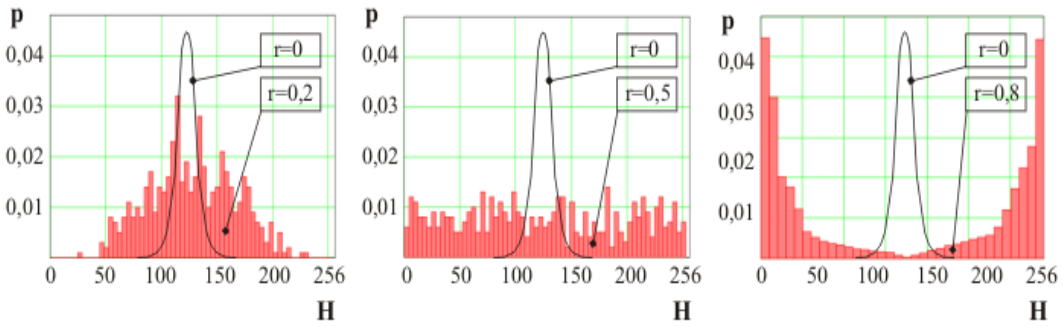

Рисунок 4 – Эволюция гистограмм распределений меры Хемминга при зависимых входных биометрических данных (линией условно обозначено распределение для независимых входных данных)

Точное «аналитическое» описание биномиального закона распределения значений [2] существует только для независимых состояний кодов. Для зависимых коррелированных состояний кодов биномиальный закон на данный момент не определен. Соответственно, его определение может быть выполнено численным моделированием простейших однослойных нейросетевых преобразователях биометрия/код. Имея технологию обучения нейросетевых преобразователей биометрия/код, мы можем варьировать коррелированность входных данных и тем самым численно получать распределения мер Хемминга выходных кодов разной степени взаимосвязанности. Мы получили возможность провести численное экспериментирование на больших выборках и получить с требуемой точностью любую из гистограмм зависимого биномиального закона распределения дискретных состояний.

С практических позиций наибольший интерес представляет моделирование зависимого биномиального закона распределения при равновероятных состояниях выходных разрядов кодов в интервале модулей коэффициентов корреляции в интервале от 0 до 0.25. Численный эксперимент показал, что семейство зависимых биномиальных законов хорошо аппроксимируется суперпозицией нормального и равномерного закона распределения. Такая аппроксимация отображена на рисунке 5.

Выбор такого типа аппроксимации обусловлен тем, что, как видно из рисунка 4, идеальный нормальный закон распределения с ростом корреляционной связи увеличивает свою дисперсию и постепенно превращается в идеальный равномерный закон распределения. Соответственно, подбирая весовые коэффициенты при этих законах, мы имеем возможность получить их удачную аппроксимацию.

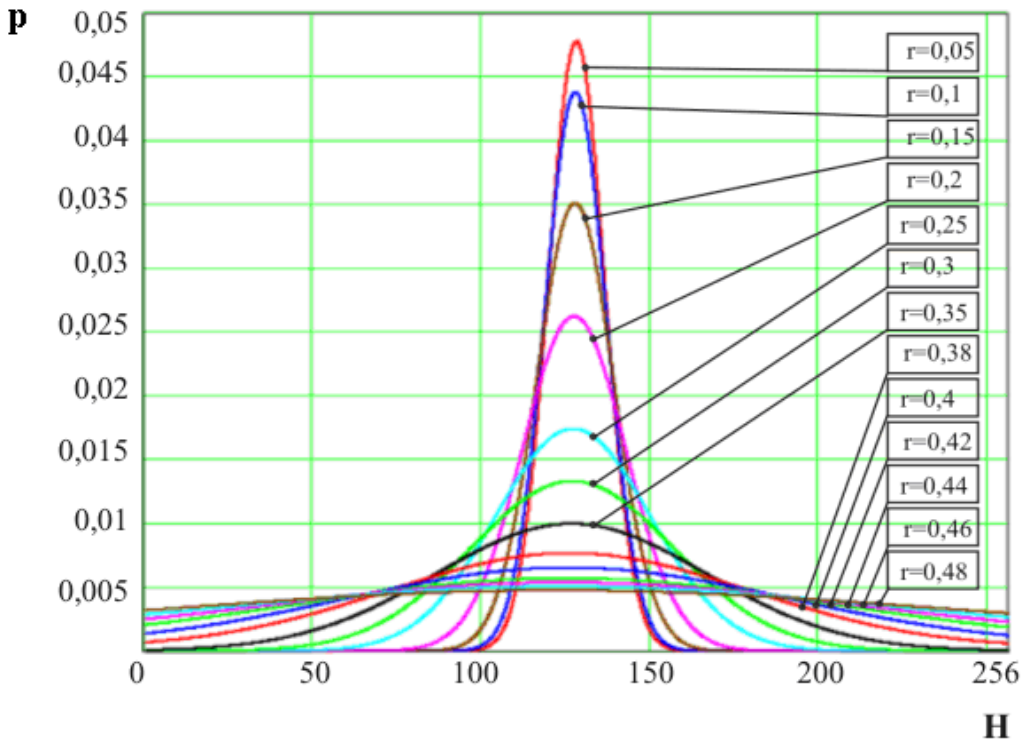

Рисунок 5 – Приближение закона распределения для зависимых данных с коэффициентом корреляции от r=0.05 до r=0.48

При модуле коэффициента корреляции, равном 0.5, биномиальный зависимый закон распределения совпадает с равномерным законом распределения. При дальнейшем росте значений модуля коэффициентов корреляции центр закона распределения опускается, и его края поднимаются, как это показано на рисунке 6.

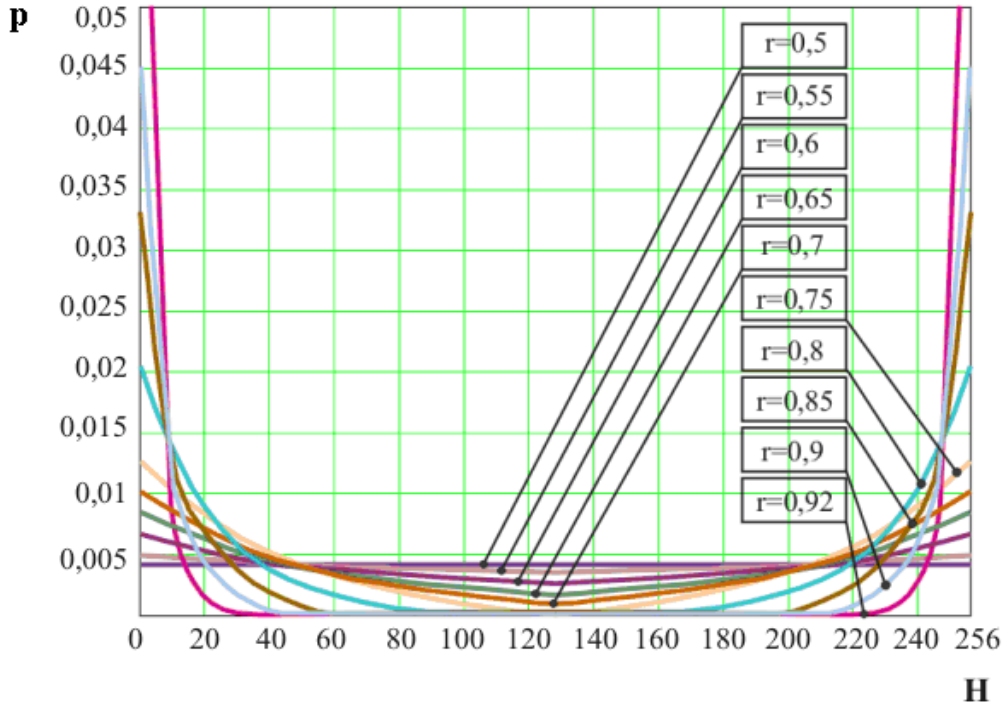

Рисунок 6 – Приближение закона распределения для зависимых данных с коэффициентом корреляции от r =0.54 до r =0.92

Получается совершенно иной тип семейства кривых. Как показала практика, хорошей аппроксимацией вогнутого по центру семейства законов распределения является степенной ряд суперпозиции нормального и равномерного законов распределений. Этот же тип аппроксимации удобен для описания сильно коррелированных кодов откликов на образы «Свой», что отображено в левой части рисунка 6.

Численный синтез гистограмм всего семейства зависимых биномиальных законов распределения значений, видимо, может иметь определенную научную значимость для теоретической статистики. Для практических нужд тестирования высоконадежных средств биометрико-криптографической защиты [1] нет необходимости в наличии полных таблиц распределений. Для удовлетворения первостепенных нужд практического тестирования вполне достаточно ряда частных таблиц описания системы, соответствующих двум предельным случаям:

1) для неизвестного «Чужому» (нескомпрометированного) биометрического образа «Свой» (смотри распределения в центральной части рисунка 7.);
2) для полностью скомпрометированного биометрического образа «Свой» (смотри распределения в левой части рисунка 7).

На первых порах вполне можно обойтись без промежуточных распределений зависимых выходных кодов.

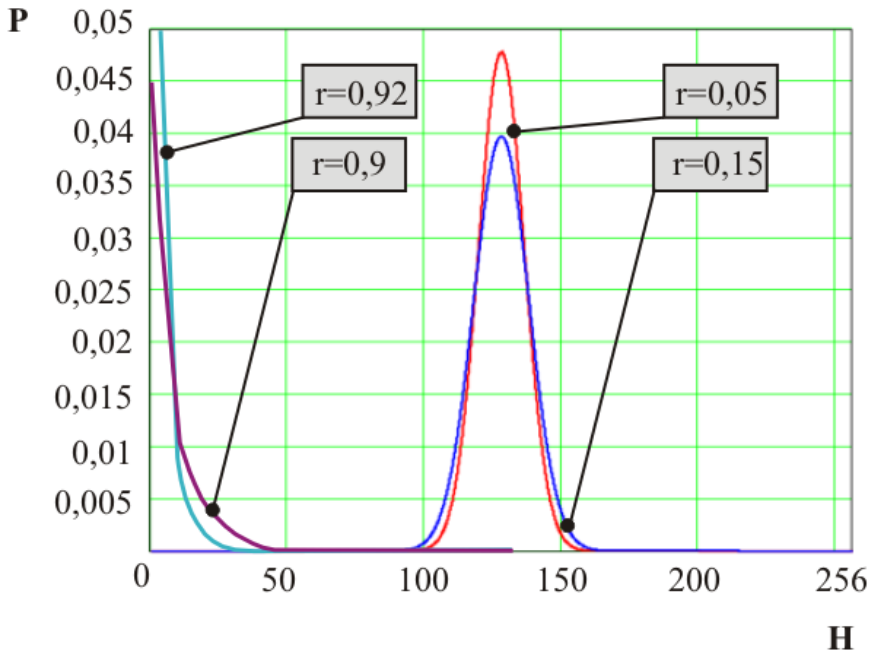

Рисунок 7 – Приближение закона распределения для зависимых данных «СВОЙ» с коэффициентом корреляции от r=0.9, r=0.92

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. Боровиков В. STATISTICA: искусство анализа данных на компьютере. Для профессионалов – СПб.: Питер, 2001 – 656 с.: ил.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.46-49. Секция-2: Информационная безопасность сложных систем.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/012)

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ «ЦИФРОВОГО РАВЕНСТВА» НА ОСНОВЕ РАЗВИТИЯ ТЕХНОЛОГИИ БИОМЕТРИКО-НЕЙРОСЕТЕВЫХ ПРЕОБРАЗОВАНИЙ

Захаров О.С., Иванов А.И., Фунтиков В.А., Ефимов О.В.
Пенза, ФГУП «ПНИЭИ»

В настоящее время наблюдается стремительная информатизация общества. Данный процесс приводит к появлению и дальнейшему расширению “цифрового неравенства”. Проблему “цифрового неравенства” можно рассматривать в нескольких аспектах. Интересно, что в Европейских странах не рассматриваются глубинные аспекты этого явления, говорится только о доступности Интернета для широких слоёв населения, о возможности голосовать не выходя из дома и тому подобных вещах. Однако, реальное “цифровое равенство” – это не только свободный доступ в Интернет, но и равные цифровые права всех членов общества.

Например, если рассматривать цифровые права банкира и домохозяйки, то юридически они равны, однако практически это далеко не так. Доверие к электронной цифровой подписи банкира намного выше доверия к ЭЦП домохозяйки. Это связано с тем, что у банкира есть сейф, охрана, таким образом, он может обеспечить надежное хранение своего личного криптографического ключа, формирующего электронную цифровую подпись электронного документа. В отличие от банкира, ключ формирования ЭЦП которого всегда хранится в сейфе, домохозяйка не может себе этого позволить. Её ключ ЭЦП, скорее всего, будет храниться в сумочке, что автоматически ставит домохозяйку в более уязвимое положение.

Именно это обстоятельство и называется действительным “цифровым неравенством”, когда декларированная для всех одинаковая юридическая значимость электронной цифровой подписи на деле будет иметь разный уровень доверия.

Ликвидировать подобное неравенство может только государство, предпринимая специальные меры, уравнивающие цифровые права всех граждан не зависимо от их социального статуса. Предвидя возникновение и усиление «цифрового неравенства» государству необходимо создавать специальные механизмы, сглаживающие изначальное неравенство.

Существуют различные способы решения данной задачи. Например, государство может обеспечить всех своих граждан специальными надежными и мобильными средствами хранения конфиденциальной информации. В качестве такого надежного средства хранения может быть использован специализированный нейросетевой контейнер. Нейросетевой контейнер – это программа, способная преобразовывать легко запоминаемый человеком пароль в криптографический ключ ЭЦП или очень длинный обычный пароль доступа. В качестве легко запоминаемого пароля может использоваться рукописная или голосовая фраза-пароль. Всё зависит от конкретной реализации.

На рисунке 1 приведён пример такого нейросетевого контейнера. Данная программа преобразовывает рукописный пароль пользователя в его личный ключ.

Действительный хозяин этой программы (хозяин упакованного в нее ключа) всегда может извлечь ключ из нейросетевого контейнера, так как он

помнит свой пароль и умеет воспроизводить свой почерк (свою уникальную динамику почерка). На рисунке показан пример извлечения легальным пользователем длинного ключа длиной 256 символов из короткого парольного слова “*Пенза*”.

Таким образом, человеку не нужно запоминать огромные последовательности символов (длинные пароли) или записывать свой ключ на бумагу. Имея при себе такой контейнер, пользователь всегда сможет получить свой ключ или длинный пароль, что избавляет его от необходимости иметь специальный сейф или охрану.

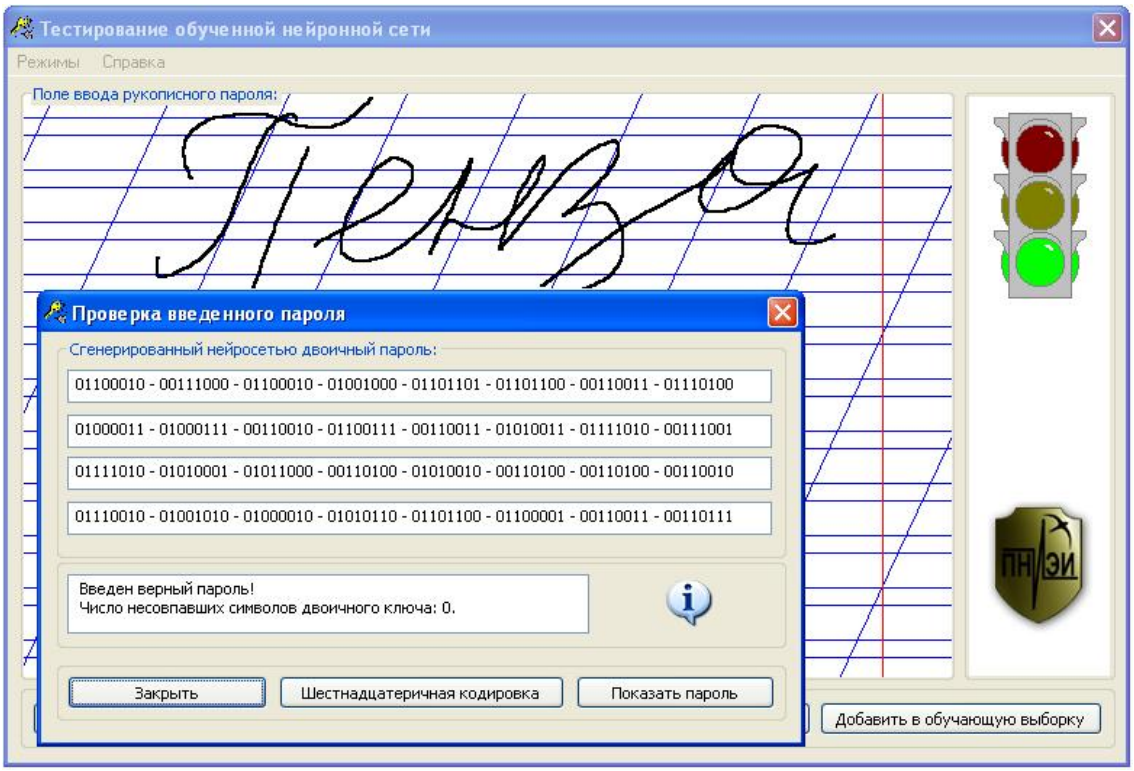

Рисунок 1 – Пример получения легальным пользователем криптографического ключа длиной 256 бит

Главным достоинством нейросетевых хранителей паролей является невозможность извлечения нелегальным пользователем (“чужой”) личного ключа легального пользователя, то есть нелегально извлечь из программы рукописный пароль или ключ пользователя практически невозможно. Для получения личной информации легального пользователя “чужой” будет вынужден перебирать все возможные варианты рукописных паролей, что является задачей сопоставимой по сложности с подбором криптографического ключа.

На рисунке 2 показана попытка “чужого” извлечь личный ключ “своего”, предъявляя случайные рукописные образы. Для получения правильного ключа необходимо будет перебрать около 10^{12} вариантов рукописных образов. Более того, для каждого пользователя создается уникальный биометрический замок (уникальна и никогда не повторится структура нейросети, генерируемой программой). Это является гарантией того, что опыт, полученный злоумышленниками при взломе имеющегося у них какого-либо другого замка, будет бесполезен, когда они начнут ломать конкретный замок. Таким образом, использование нейросетевых контейнеров может способствовать преодолению “цифрового неравенства”.

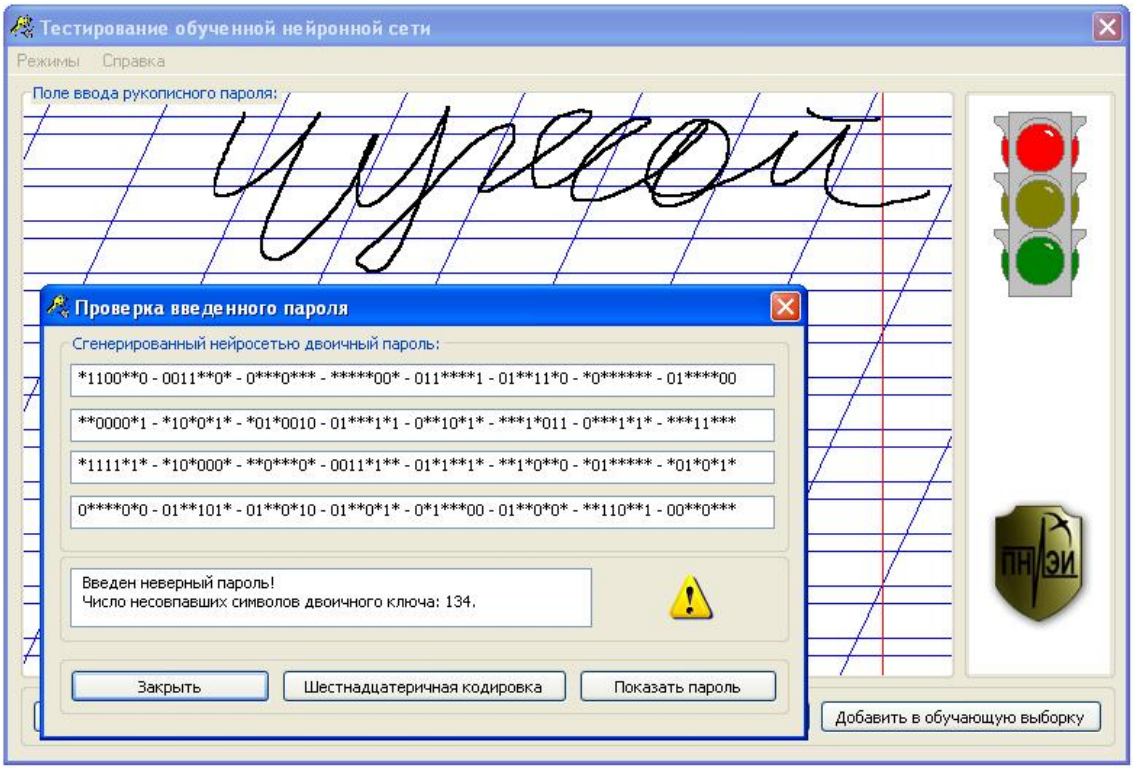

Рисунок 2 – Пример попытки нелегального извлечения ключа (символ * отражает не совпавшие биты правильного и полученного ключа)

Исследования российских специалистов показали, что надежность подобной технологии оказывается очень высокой, если пользователь сохраняет свой биометрический образ (например, рукописный пароль) в тайне. Если же этого не делать и использовать, например, свой открытый автограф, то стойкость биометрической защиты резко падает. В этом случае мы приходим к достаточно “слабым” биометрическим технологиям защиты, активно рекламируемым на западе и востоке. Биометрия открытых образов будь то отпечатки пальцев, геометрия лица, радужная оболочка глаза и т.п. крайне уязвима по отношению к атакам профессионалов и сама нуждается в защите. Верить рекламным заявлениям зарубежных производителей нельзя. Необходимо иметь свои испытательные лаборатории биометрических средств защиты, свои методики тестирования, свою систему нормативно правовых документов, регламентирующих требования к тем или иным биометрическим технологиям.

В России активно идет процесс создания нормативно-технической базы, так ГОСТ Р ТК355 ПК7 адаптирует к русскому языку международные биометрические стандарты, созданные под систему международных паспортов с биометрическими механизмами идентификации человека. В 2005 году переведено два международных стандарта из более чем тридцати планируемых к введению в ближайшее время международным комитетом ISO/IEC JTC1 SC37.

За международную стандартизацию биометрии, стыкующейся с криптографией, отвечает ISO/IEC JTC1 SC27 (наш аналог ГОСТ Р ТК362). Пока подкомитет SC27 не объявил о своей решимости создать международный стандарт, регламентирующий требования к биометрическим хранителям личных секретов частных граждан.

Подчеркнем, что работы по преобразованию биометрического образа человека в его ключ ведутся не только в России. Подобные работы ведутся во всех странах, имеющих сколько ни будь значимый научный потенциал. Открыто публикуют свои результаты две страны это США и Россия. Подходы к решению

задачи у этих двух мировых лидеров существенно разные. Исследователи университетов США [1] предлагают мировому сообществу идти по пути использования нечеткой, размытой «fuzzy» математики. В России для той же цели предлагается использовать обучение больших и сверхбольших искусственных нейронных сетей [2]. Какой из этих двух путей развития в ближайшем будущем окажется более востребованным мировым сообществом пока не ясно. В этом плане проект национального стандарта [2] создан с учетом возможного появления на нашем рынке обоих типов средств биометрико-криптографической защиты информации.

Начало публичного обсуждения проекта национального российского стандарта [2] является знаменательным событием. То, что Россия раньше своих соседей по Европе и США имеет эффективные механизмы противодействия “цифровому неравенству” позволяет ей уже сейчас правильно закладывать фундамент будущей информационной безопасности. При закладке фундамента безопасности будущей информационной России точно повторять решения Европы и США нельзя. Уже сейчас видно, что их технические решения по биометрической защите очень дороги и крайне уязвимы. Мы не так богаты как они. Нам нужны менее дорогие, но гораздо более эффективные технические решения. Имеет прямой смысл тратить национальные ресурсы на свои биометрические паспорта и удостоверения личности учитывать не только требования международных биометрических стандартов, но и требования своего собственного национального стандарта [2]. Более того, имеет смысл продвигать Российский национальный стандарт [2] как международный, через соответствующие подкомитеты ISO/IEC JTC1.

Подытоживая вышесказанное, необходимо отметить, что в настоящее время в России начали появляться надежные нейросетевые хранители биометрической и конфиденциальной криптографической информации. Для обеспечения не только юридического, но и реального “цифрового равенства” необходимо способствовать дальнейшему развитию и продвижению подобных нейросетевых хранителей. Возможны два пути развитии нейросетевых технологий. Первый путь, когда всё финансовое бремя ложится на плечи конкретных пользователей, в данном случае существует вероятность затягивания перехода на новую технологию на неопределённый срок. Второй путь, когда все первоначальные затраты на развитие и продвижение новых технологий берет на себя государство. Государству выгоднее своевременно позаботиться о создании безопасной среды, чем в дальнейшем бороться со злоупотреблениями.

ЛИТЕРАТУРА:

1. Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data /Yevgeni Dodis, Leonid Reyzin, Adam Smith //April 13, 2004. www.cs.bu.edu/~reyzin/fuzzy.html
2. Первая редакция проекта ГОСТ Р (ТК 362) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005. 32 с. Публичное обсуждение начато с 9.09.05.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.50-52. Секция-2: Информационная безопасность сложных систем.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/013)

ПРЕИМУЩЕСТВА НАЦИОНАЛЬНОГО РОССИЙСКОГО ПОДХОДА К БЕЗОПАСНОМУ ОБЪЕДИНЕНИЮ МЕХАНИЗМОВ БИОМЕТРИИ И КРИПТОГРАФИИ

Ефимов О.В., Иванов А.И.
Пенза, ФГУП «ПНИЭИ»

Информатизация общества приводит к широкому распространению средств защиты информации. Наиболее эффективными являются средства криптографической защиты информации. Фактически информационное общество может быть устойчивым только при тотальном, массовом использовании криптографических механизмов защиты информации [1]. Классическая криптография способна обеспечить любую стойкость защиты при незначительном потреблении вычислительных ресурсов, однако для обеспечения ее эффективности необходимо надежно хранить личные криптографические ключи граждан информационного общества. Безопасное хранение криптографических ключей обычных граждан не может осуществляться традиционными методами и является одной из важнейших проблем развития будущего информационного общества.

Одним из путей решения этой задачи является использование самого человека (его биометрии) для организации доступа к его личной криптографической информации. Предполагается создание некоторых преобразователей биометрии человека в его личный ключ. Например, в России развивается технология нейросетевого преобразования биометрии человека в его личный ключ. Наиболее надежными в данный момент являются нейросетевые преобразователи рукописного пароля в криптографический ключ или длинный пароль. На рисунке 1 поясняется принцип нейросетевого преобразования рукописного пароля в личный ключ.

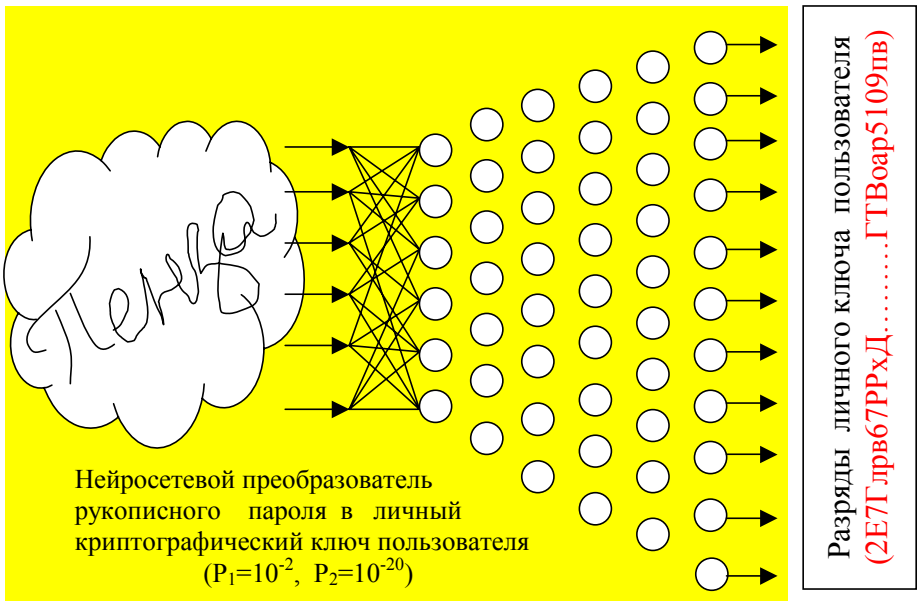

Рисунок 1 – Нейросетевой преобразователь нечеткого биометрического образа человека в его однозначный криптографический ключ

Очевидно, что наиболее сложной является не сама задача нейросетевого преобразования, а задача обучения большой нейронной сети такому преобразованию. Проблема усложняется тем, что обучение должно быть автоматическим. В соответствии с российской технологией для обучения используются несколько примеров биометрического образа «Свой» и множество образов «Чужих». Процедура автоматического обучения поясняется рисунком 2.

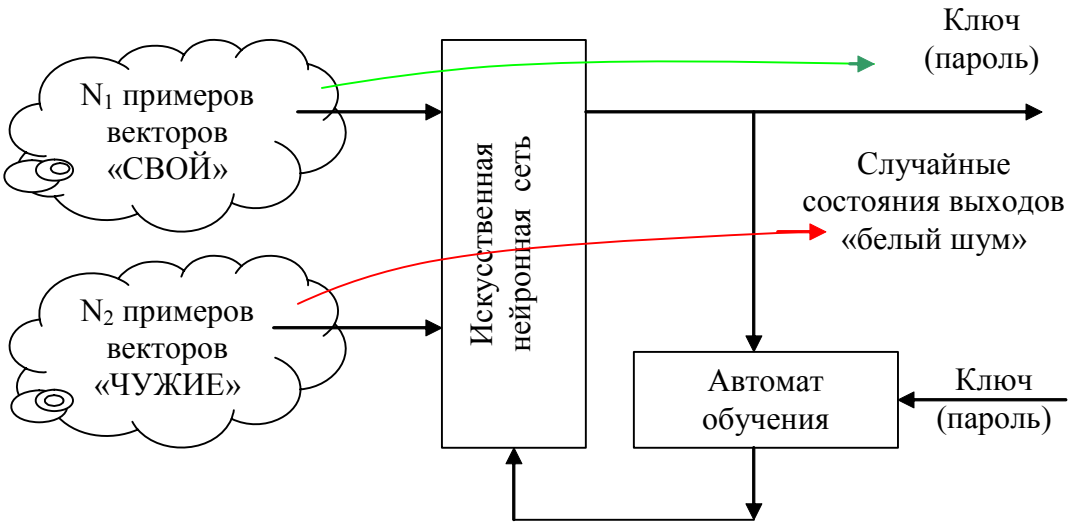

Рисунок 2 – Обучение нейросетевого преобразователя

Подчеркнем, что работы по преобразованию биометрического образа человека в его ключ ведутся не только в России. Подобные работы ведутся во всех странах, имеющих сколько ни будь значимый научный потенциал. Открыто публикуют свои результаты две страны это США и Россия. Подходы к решению задачи у этих двух мировых лидеров информационной защиты существенно разные. Исследователи университетов США [2] предлагают мировому сообществу идти по пути использования нечеткой, размытой «fuzzy» математики. В России для той же цели предлагается использовать обучение больших и сверхбольших искусственных нейронных сетей. Какой из этих двух путей развития в ближайшем будущем окажется более востребованным мировым сообществом пока не ясно. В этом плане проект национального российского стандарта [3] создан с учетом возможного появления на нашем рынке обоих типов средств биометрико-криптографической защиты информации.

Результаты сопоставительного сравнения двух путей развития информационной безопасности больших и сверхбольших систем приведены в таблице 1.

Из приведенной ниже таблицы следует, что на данный момент путь, предлагаемый мировому сообществу Россией, более детально проработан. По крайней мере, заявляемые характеристики отечественных нейросетевых преобразователей могут быть оценены не только теоретически, но и экспериментально. Немаловажным является так же то, что с 9 сентября 2005 года в России начато публичное обсуждение проекта национального стандарта по требованиям к высоконадежным средствам биометрической защиты [3]. Этот факт косвенно подтверждает преимущества пути развития средств высоконадежной биометрии, предлагаемый Россией.

Таблица 1

N	Параметр сравнения	Результаты сравнения технологий двух стран	
		РОССИЯ	США
1	Тип преобразователя	Нейросетевая хэш-функция	«Fuzzy» хэширование
2	Наличие внешнего ключа	Ключевое хэширование	Безключевое хэширование
3	Вычислительная сложность синтеза преобразователя	Квадратичная	Полиномиальная
4	Время синтеза (обучения) преобразователя	30 секунд	Нет данных
5	Уровень автоматизации синтеза (обучения) преобразователя	Полная автоматизация	Нет данных
6	Наличие действующих макетов, опытных образцов	ЕСТЬ	Нет данных
7	Наличие национального стандарта по требованиям к преобразователям	ЕСТЬ	НЕТ

В итоге мы можем констатировать существенное отставание России по обычным биометрическим технологиям (распознаванию глазного дна, отпечатков пальцев, геометрии руки, кровеносных сосудов глазного дна) из-за экономических потрясений в течение последних 15 лет. Однако это касается только относительно слабых биометрических технологий общего применения. Именно по этой причине в США уже разработан ряд национальных биометрических стандартов, которые в данный момент проводятся ISO/IEC JTC1 SC37 как международные стандарты. Что касается технологий разработки высоконадежной биометрико-криптографической аутентификации, то Россия по этим технологиям двойного применения имеет хорошие позиции и вполне может предложить свой национальный стандарт [3] как основу для соответствующего международного стандарта. Теория подобных технологий достаточно хорошо отработана [4].

ЛИТЕРАТУРА:

1. Гезенко И.И., Иванов А.И. Обеспечение устойчивости будущего информационного общества: массовая гражданская криптография. //Защита информации. *Inside*. 2005, №1.
2. Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data /Yevgeni Dodis, Leonid Reyzin, Adam Smith //April 13, 2004. www.cs.bu.edu/~reyzin/fuzzy.html
3. Первая редакция проекта ГОСТ Р (ТК 362) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005. 32 с. Публичное обсуждение начато с 9.09.05.
4. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Издательство Пензенского государственного университета – 2005 г.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.53-59. Секция-2: Информационная безопасность сложных систем.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/014)

ТЕХНИЧЕСКИЕ СРЕДСТВА МОБИЛЬНОГО ХРАНЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЯ НА БАЗЕ ПОРТАТИВНЫХ «ФЛЭШПРОЦЕССОРОВ» И ИХ ПРИМЕНЕНИЕ В КОРПОРАТИВНЫХ СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Колючкин А.В., Трифонов С.Е.
Пенза, ФГУП «ПНИЭИ»

В настоящее время в нашей стране идет бурный процесс информатизации практически всех сфер общественной деятельности. Хотя бумажный документооборот все еще преобладает над электронным документооборотом в силу довольно слабой распространенности последнего среди массового потребителя, 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.

В настоящее время предприятие ФГУП «ПНИЭИ» г. Пенза проводит ряд разработок, направленных на создание изолированной программно-аппаратной среды для выполнения функций криптографической обработки информации на базе отечественных алгоритмов. В том числе защищенные от НСД индивидуальные малогабаритные (портативные) устройства пользователя.

Малогабаритные портативные устройства представляют собой вычислительную программно-аппаратную среду на базе встроенных микроконтроллера и *Flash*-памяти большого объема (до 1024 Мбайт), имеют последовательный стык ввода/вывода USB 1.1 или 2.0. С целью защиты от НСД конструкция выполнена в виде неразборного малогабаритного корпуса с внешним разъемом USB-A.

Кроме того, в устройствах применяется ряд дополнительных технических решений, позволяющих обеспечить защиту от НСД даже в случае взлома корпуса и доступа к программно-аппаратным ресурсам устройства.

Внешний вид устройства и его габаритные размеры приведен на рисунке 1. Технические характеристики данной программно-аппаратной среды приведены в таблице 1.

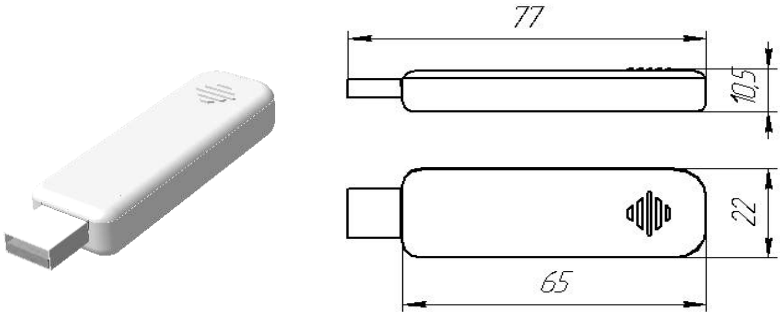

Рисунок 1 – Внешний вид устройства и его габаритные размеры

Таблица 1

Архитектура	Накопитель на базе *Flash*-памяти, работающий под управлением микроконтроллера
Исполнение	Малогабаритный корпус с USB-разъемом типа А
Емкость памяти	64, 128,256, 512, 1024 Мбайт
Материал корпуса	Пластмасса, металл (в зависимости от желания заказчика)
Тип микроконтроллера	PIC18LF4550 (в перспективе – отечественный микроконтроллер, аналогичный приведенному, со встроенным ядром криптографической обработки информации)
Тактовая частота микроконтроллера	48 МГц
Протокол обмена с устройствами	USB 1.1, интерфейс точка-точка
Скорость обмена	12 Мбит/с
Логические уровни обмена	Логические уровни USB-интерфейса
Вес, не более	20 г
Напряжение питания	5 В
Потребляемый ток, не более	100 мА
Рабочая температура	От –40 до +50°С
Температура хранения	От –55 до +65°С
Питание	От интерфейса USB
Количество перезаписей в одну ячейку памяти	Не менее 100 000
Срок хранения данных, не менее	10 лет

Данные устройства – малогабаритные вычислитель-носители (МВН) – имеют следующие функциональные характеристики:

– защита от НСД криптографическими, алгоритмическими и физическими способами;

– возможность гарантированного стирания записанной информации (как выборочно, так и в полном объеме (аварийно));

– большой объем встроенной памяти (до 1 Гбайт), позволяющий хранить не только большой объем электронной информации, но и ключевой информации пользователя (ключи (открытые и закрытые) электронной цифровой подписи (ЭЦП) [1], сертификаты открытых ключей ЭЦП).

Созданный и рассмотренный задел может быть значительно расширен как функционально, так и по назначению.

Например, ФГУП «ПНИЭИ» проработаны технологии встраивания в защищенную программно-аппаратную среду МВН (без увеличения его массо-габаритных характеристик) средств криптографического преобразования информации с аппаратной поддержкой для достижения высоких показателей производительности, включая алгоритм шифрования ГОСТ 28147-89 [2], алгоритм вычисления хэш-функций от сообщений произвольной длины согласно ГОСТ Р 34.11-94 [3] и алгоритм ЭЦП согласно ГОСТ Р 34.10-2001 [1].

Примерный перечень основных функциональных характеристик, которые могут быть обеспечены МВН [5]:

– обеспечение криптографической защиты информации пользователя (группы пользователей) в виде файлов или данных, а также защиты от несанкционированного доступа (НСД) к ресурсам и записанной информации с помощью пароля;

– вычисление хэш-функции согласно ГОСТ Р 34.11-94 [3];

– вычисление электронной цифровой подписи согласно ГОСТ Р 34.10-2001 [1];

– обеспечение криптографических преобразований по алгоритму шифрования согласно ГОСТ 28147-89 [2];

– поддерживаемые платформы: Windows 9x/2000/XP, Linux, МСВС 3.0, DOS 6.22;

– наличие встроенной системы организации файлов;

– возможность внутреннего 100% резервирования программно-аппаратной среды.

– Благодаря этому возможны следующие модификации МВН по назначению:

– МВН аутентификации пользователя по паролю и определения выделенных каждому пользователю полномочий;

– МВН хранения ключей пользователя в защищенной среде с доступом по паролю;

– МВН индивидуальной криптографической защиты информации пользователя с возможностью шифрования/дешифрования файлов и данных пользователя в режимах как «на проходе» (ПЭВМ⇒Носитель⇒ПЭВМ), так и в режимах с сохранением информации в физически защищенной от НСД среде МВН в зашифрованном виде.

– Показатели производительности МВН:

– производительность шифрования информации – не менее 500 - 600 кбайт/с;

– производительность хэширования информации – не менее 300 кбайт/с;

– время вычисления ЭЦП – не более 1,2 сек;

– время проверки ЭЦП – не более 2,4 сек;

– ресурс формирования ключевых пар (ключ ЭЦП и ключ проверки ЭЦП) – 2 млн. пар.

Начиная с 2001 г. на предприятии ведутся исследования по биометрической идентификации личности с применением технологий искусственных нейросетей. При этом проблемы биометрии на предприятии рассматриваются в непосредственной взаимосвязи с методами криптографической защиты на базе отечественных алгоритмов.

Кроме того, ФГУП «ПНИЭИ» принимает непосредственное участие в разработке проекта ГОСТ [4] «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации».

В настоящее время ФГУП «ПНИЭИ» прорабатывает варианты встраивания нейронных сетей в изолированную программно-аппаратную среду МВН в целях внедрения передовых биометрико-криптографических технологий высоконадежной аутентификации и авторизации пользователей в соответствии с их биометрическими параметрами, включающими тайный образ [5]. При этом сам пользователь является носителем криптографического ключа, а доступ его к ресурсам МВН может быть осуществлен только после предъявления биометрических параметров (речь, отпечатки пальцев).

Это направление ФГУП «ПНИЭИ» рассматривает в качестве перспективного и провел изготовление действующего макетного образца. На рисунке 2 приведены эскизы трех возможных модификаций данных устройств.

Рисунок 2 – Эскизы трех модификаций флэшпроцессоров

Применение выше описанных МВН в системах управления обменом электронной информацией с юридически значимой ЭЦП [1], к которым предъявляются требования информационной безопасности, позволяет достигнуть качественно новых тактико-технических показателей [5].

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.

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.

Рассмотрим подробнее вопрос применения МВН в системах управления электронным документооборотом и проблемы обеспечения безопасности в ЭДО с применением подобных изделий.

Под управлением электронным документооборотом в общем случае понимают весь комплекс процедур по организации составления, использования, хранения и обмена электронными документами.

Для создания и поддержания инфраструктуры электронного документооборота с ЭЦП, имеющей юридическую значимость, федеральный закон (ФЗ) [6] «Об электронной цифровой подписи» требует наличия третьей «арбитражной» доверенной для всех участников стороны – Удостоверяющего Центра (УЦ).

Основными функциями УЦ должны явиться:

– автоматизированное управление политикой безопасности, включая управление ключами и сертификатами участников;

– управление индивидуальной (персональной) информацией участников;

– удостоверение подлинности ЭЦП [1];

– 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 в том или ином ведомстве.

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.

Другими словами, инфраструктура открытых ключей есть система цифровых сертификатов, центров сертификации и других регистрационных центров, которые проверяют и идентифицируют каждую из сторон, вовлеченных в электронный информационный обмен, реализуя "иерархию доверия”.

Естественным требованием является то, что технология использования открытых ключей, применяемых в ЭЦП, должна интегрировать все функциональные области системы безопасности информации, соответствующей заданному уровню доверия.

Применительно к задачам организации сбора и обмена информацией в инфраструктурах открытых ключей следует обратить внимание, что большое значение должно иметь выполнение двух условий. С одной стороны, система безопасности должна обеспечивать необходимый уровень защищенности электронного информационного обмена, гарантирующего безопасность при всех видах атак как со стороны внешнего, так и внутреннего нарушителя. В то же время, наличие интегрированной подсистемы безопасности в системе электронного информационного обмена не должно приводить к усложнению работы пользователя, когда на него возлагается значительная часть управления безопасностью. Это создает большой ряд угроз информационной безопасности, но может также привести и к сбоям (системным отказам) в процессе электронного информационного обмена по вине пользователя.

Таким образом, имея в виду информационные системы с ЭДО с применением ЭЦП, в современной трактовке требование обеспечения защиты соответствующего уровня предполагает наличие подсистемы автоматизированного управления безопасностью, включая дистанционное управление шифрключами, ключами ЭЦП и сертификатами по каналам связи в режимах «прозрачных» для пользователей. Поэтому на УЦ в системе ЭДО должны быть возложены дополнительные функции автоматизированного управления безопасностью. Только при выполнении этого требования могут быть созданы условия «погружения» технологий ЭЦП и функций УЦ в безопасную среду, стойкую к атакам квалифицированного нарушителя. При этом следует иметь в виду, что особый класс нарушителя в системе ЭДО, имеющий значительный перечень существующих угроз безопасности, составляют внутренние нарушители, являющиеся пользователями системы и образовавшиеся вследствие явных и неявных компрометаций.

Указывая на интегрированный характер подсистемы обеспечения безопасности информации, необходимо обратить внимание также на следующий факт: подсистема безопасности, опираясь на единое ядро криптографической защиты, должна охватывать несколько уровней сетевого взаимодействия. Как показывает практика, минимально необходимыми в этом отношении являются прикладной (пользовательский) уровень и уровень сетевого управления (сетевой).

Для решения задачи НСД к информационным ресурсам и службам УЦ, а также в целях автоматизации процесса учета событий и организации аудита

безопасности на заданную глубину во времени, в защищенной среде ЭДО должны быть выполнены три условия.

Во-первых, должна быть обеспечена доверенная и защищенная от НСД программно-аппаратная среда для каждой компоненты УЦ;

Вторым условием является персонализация всех действий обслуживающего персонала и администраторов по управлению УЦ на всех территориально-распределенных объектах с введением автоматизированного учета событий, защищенного от модификаций и несанкционированного уничтожения;

В третьих, особую проблему составляет задача создания подсистемы управления ключами в защищенной системе электронного документооборота с применением ЭЦП. В целях обеспечения оперативности функционирования и живучести в системе должны быть предусмотрены технические решения, обеспечивающие как клиентские рабочие места ЭДО, так и компоненты УЦ возможностями децентрализованной генерации ключей ЭЦП (пар ключей ЭЦП: открытый ключ/закрытый ключ).

Таким образом, в целях эффективного решения рассмотренных вопросов и обозначенных проблем безопасности как внутри инфраструктуры УЦ, так и на клиентских рабочих местах ЭДО целесообразно применять СКЗИ, выполненные на базе изолированной, малогабаритной, многофункциональной, защищенной от НСД среды. Созданный ФГУП «ПНИЭИ» задел может быть также эффективно использован в целях создания УЦ и оснащения клиентских рабочих мест.

Большую актуальность при внедрении юридически значимой ЭЦП с электронным документооборотом имеет задача сопряжения с действующими системами электронного документооборота. Эта проблема может быть эффективно решена опять же с помощью клиентских МВН, реализующих функции криптопровайдера и выполненных в виде выделенной от абонентских станций изолированной программно-аппаратной среды.

Отличительной особенностью действующей системы юридически значимого ЭДО с применением МВН-криптопровайдера является то, что все процессы криптографической обработки электронных документов осуществляются в изолированной и защищенной от НСД программно-аппаратной среде криптопровайдера, отделенной от общесистемной и операционной среды ПЭВМ или сопрягаемых изделий. Кроме того, шифрключи, включая ключи шифрования и ключи ЭЦП, никогда не покидают и не выводятся за пределы программно-аппаратной среды криптопровайдера в течение всего жизненного цикла и неизвестны даже пользователю СКЗИ.

Второй отличительной особенностью данного технического решения является то, что каждый абонент электронной почты или электронного документооборота может на рабочем месте произвольно во времени генерировать и менять ключи ЭЦП и может быть при этом уверен, что секретные ключи вычисления ЭЦП неизвестны никому, включая УЦ. Парадокс заключается в том, что секретный ключ вычисления ЭЦП остается неизвестным даже самому пользователю – ключ формируется и функционирует только в изолированной среде криптопровайдера, недоступной пользователю для непосредственного обращения.

В третьих, принципиально важной тактико-технической характеристикой рассматриваемых технических решений, опять-таки в силу изолированности среды, отделенной от общесистемной среды ПЭВМ, является возможность достижения высоких уровней защищенности при минимальных затратах средств и времени на разработку. При этом практически не затрагивается операционная среда ПЭВМ и выполняемых в ней приложений. Например, ФГУП «ПНИЭИ»

прорабатывает вопрос использования криптопровайдера в среде приложений электронного документооборота *Lotus Notes* или *MS Docs Vision* [5] для вычисления юридически значимой ЭЦП согласно отечественного криптографического алгоритма. При этом предполагается, что вся криптографическая обработка данных должна проходить в режимах «прозрачных» для пользователей.

В комплексе, по мнению ФГУП «ПНИЭИ», описанные технические решения на базе изолированной, малогабаритной, многофункциональной, защищенной от НСД среды, позволят внедрить в интегрированной сети с электронным документооборотом новые принципы реализации политики безопасности с юридически значимой ЭЦП с максимальным использованием автоматизированных процессов управления и дистанционного мониторинга.

ЛИТЕРАТУРА:

1. ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Формирование и проверка электронной цифровой подписи».
2. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая».
3. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хеширования».
4. Первая редакция проекта ГОСТ Р (ТК 362) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005. 32 с. Публичное обсуждение начато с 9.09.05.
5. Отчеты НИР, ОКР.
6. Федеральный Закон «Об электронной цифровой подписи» от 10.01.2002 года №1-ФЗ.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.60-61. Секция-2: Информационная безопасность сложных систем.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/015)

ОЦЕНКА ПОГРЕШНОСТЕЙ ОПРЕДЕЛЕНИЯ СТАТИСТИЧЕСКИХ МОМЕНТОВ, ОБУСЛОВЛЕННЫХ ОТСУТСТВИЕМ ПРЕДСТАВИТЕЛЬНОЙ ВЫБОРКИ

Малыгин А.Ю., Надеев Д.Н., Иванов А.И.

Одной из проблем обучения и тестирования биометрических систем с искусственными нейронными сетями является использование непредставительных обучающих и тестовых выборок. В соответствии с общепринятой практикой доверительный интервал ошибки вычисления математического ожидания из-за непредставительности обучающей (тестовой) выборки можно вычислить, воспользовавшись распределением Стьюдента в рамках гипотезы независимости и нормальности закона распределения [1].

На рисунке 1 приведена номограмма, связывающая вероятность попадания реального значения математического ожидания μ_1 в интервал, определяемый среднеквадратическим отклонением. Применение этой номограммы эквивалентно использованию таблиц Стьюдента для оценки погрешности вычисления математического ожидания при заранее заданной доверительной вероятности.

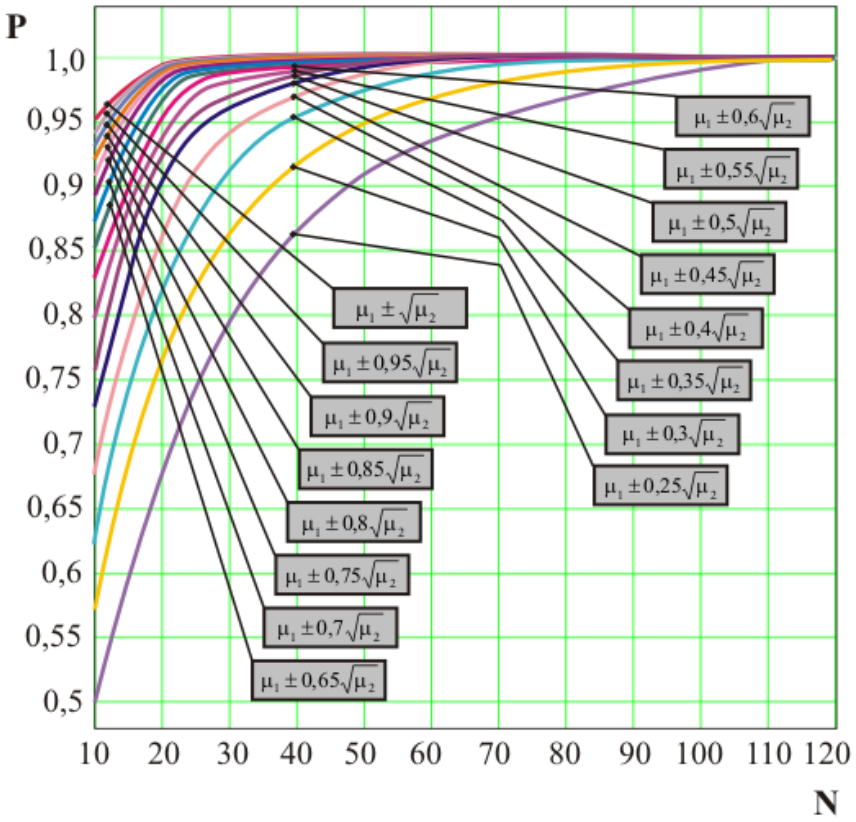

Рисунок 1 – Номограмма, связывающая вероятность попадания реального значения математического ожидания μ_1 в интервал, определяемый среднеквадратическим отклонением

Статистические моменты любого распределения значений жестко связаны с соответствующим степенным рядом, описывающим ошибки. То есть ошибку вычисления первого момента (математического ожидания) удается определить через знание значения второго момента (рисунок 1). По аналогии ошибку

вычисления второго момента или ошибку вычисления среднеквадратического отклонения можно вычислить, зная третий момент используемой непредставительной выборки. Номограмма, связывающая вероятность ошибки второго момента со значением третьего момента, приведена на рисунке 2.

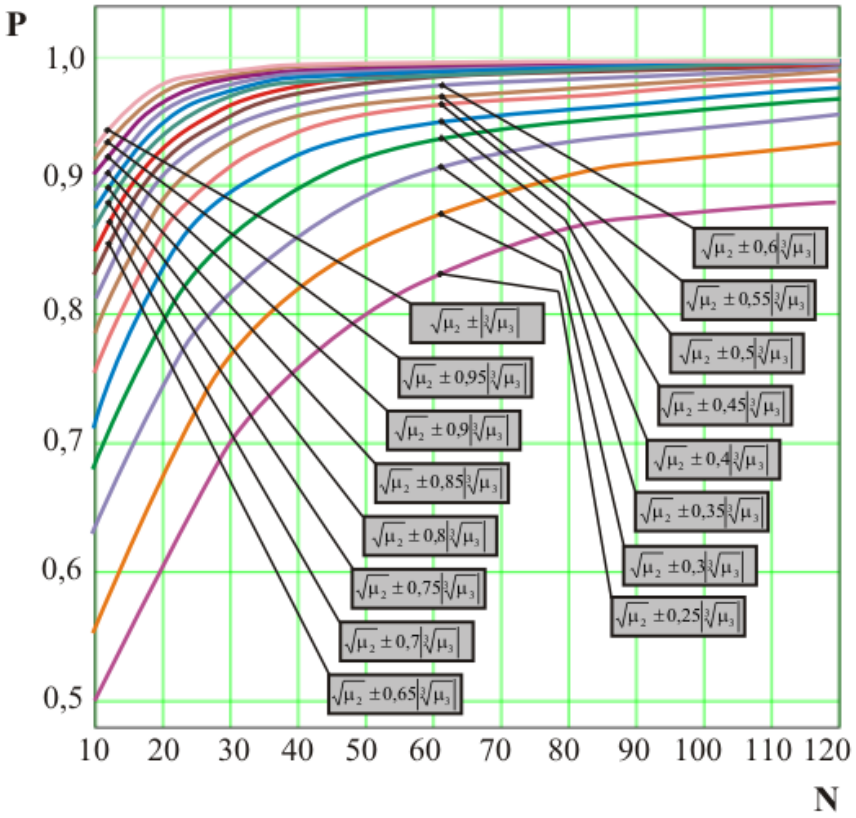

Рисунок 2 - Номограмма, связывающая вероятность попадания реального значения среднеквадратического отклонения в интервал, определяемый статистическим моментом третьего порядка непредставительной выборки

Нейросетевые преобразователи биометрия/код, выполненные в соответствии с требованиями [2], имеют практически нормальный независимый закон распределения значений выходных кодов для «Чужих», не знающих пароля. Как следствие, мы можем по гистограммам рисунков 1 и 2 вычислить значения результирующей ошибки из-за непредставительности использованной выборки. В рамках гипотезы нормального независимого закона распределения значений мы в праве говорить не об оценках стойкости нейросетевых преобразователей биометрия/код, а о статистическом измерении стойкости преобразователей к атакам подбора. Переход от оценок к измерению обусловлен возможностью вычисления ошибок из-за конечности тестовых выборок и наличию гарантий корректности гипотезы о нормальном независимом законе распределения измеряемого параметра.

ЛИТЕРАТУРА:

1. Боровиков В. STATISTICA: искусство анализа данных на компьютере. Для профессионалов. СПб: Питер–2001 г., 656 с.
2. Проект ГОСТ Р (ТК 362, первая редакция) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005 г., ФГУП ПНИЭИ, ГНИИИ ПТЗИ ФСТЭК России.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.62-64. Секция-2: Информационная безопасность сложных систем.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/016)

СОКРАЩЕНИЕ ОБЪЕМОВ ТЕСТОВЫХ ВЫБОРОК ЗА СЧЕТ ЗНАНИЯ ЗАКОНА РАСПРЕДЕЛЕНИЯ ВЫХОДНЫХ СОСТОЯНИЙ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ/КОД

Малыгин А.Ю., Иванов А.И., Надеев Д.Н.

Научное направление, связанное с аутентификацией пользователей по их биометрическим данным, в настоящее время активно развивается. Это связано с бурно растущей информатизацией общества и с появлением широкого спектра новых информационных технологий. Повышение уровня защиты биометрических средств – одна из задач, которая стоит перед производителями.

Использование многослойных нейронных сетей позволяет преобразовывать динамические биометрические образы человека, такие как рукописные слова-пароли и голосовые парольные фразы в однозначный криптографический ключ. При этом вероятность ошибки второго рода (вероятность ложного пропуска «чужого») при преобразования рукописного слова-пароля из пяти букв в ключ для среднестатистического пользователя составляет 10^{-12}, а при произнесении парольной фразы – 10^{-4} [1]. Заявляемые производителями характеристики стойкости биометрических устройств к атакам подбора требуют подтверждения. Важным положением при проведении испытаний биометрических механизмов является знание закона распределения значений выходных кодов биометрического преобразователя при атаках случайного подбора.

Предположим, что закон распределения неизвестен. При тестировании биометрических устройств с вероятностью появления ошибок второго рода $P_2 \approx 10^{-2}$ объем базы биометрических образов должен составлять $N \geq 1000$; сбор и обработка такой базы не составляет особого труда, не требуется много времени на формирование и тестирование с использованием этой базы.

Положение резко меняется, когда заявленная ошибка второго рода $P_2 \approx 10^{-12}$, тогда объем базы биометрических образов должен составлять $N \geq 10^{13}$: сбор и обработка биометрической базы рукописных образов объемом 10^{13} (ввод одного образа – 40 секунд) – $1{,}3 \cdot 10^7$ лет. Ресурсы обычных вычислительных машин позволяют эмулировать 3000 сетей в секунду при атаках на белом шуме, обрабатывать порядка 30 образов в секунду при извлечении из них 416 коэффициентов Фурье на коррелированных данных (данные программного продукта «Нейрокриптон 1.1»). При такой производительности на обычной вычислительной машине потребуется 10 лет на перебор 10^{12} возможных вариантов при эмуляции атак «белого шума». На эмуляцию атак коррелированными данными потребуется 1000 лет.

Высоконадежные биометрические устройства со стойкостью 10^{-12} и выше проще создать, чем доказательно проверить их стойкость прямым численным экспериментом. Для разрешения этого вопроса необходимо создавать и исследовать реальные базы биометрических образов достаточно больших размеров, для чего необходимы людские, финансовые, ресурсы времени и вычислительных машин; искусственными синтезированными базами не обойтись. Исследования, проведенные в лаборатории биометрических и нейросетевых технологий ПНИЭИ и лаборатории тестирования биометрических устройств и технологий при ФВО ПГУ, показали, что для больших баз биометрических

образов, собранных по специальным методикам [2], закон распределения близок к нормальному [3].

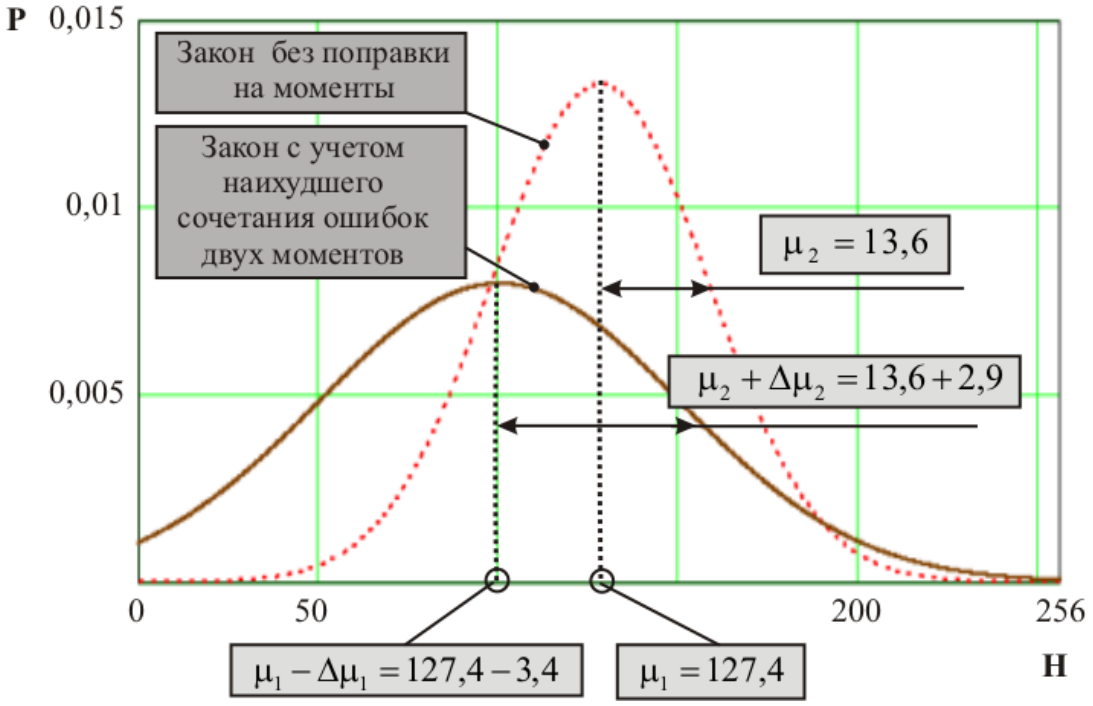

Рисунок 1 – Смещение закона, описывающего распределение выходных состояний преобразователя, полученное добавления ошибок определения двух первых моментов

Из теории математической статистики известно, что «идеальный» нормальный закон определяется двумя первыми моментами – μ_1 и μ_2. Зная их, нетрудно рассчитать необходимый минимальный размер баз биометрических образов при условии, что в генеральной совокупности рассматриваемый признак действительно распределен по нормальному закону [4].

Пример на рисунке 1 показывает изменение параметров закона из-за ошибок в расчете μ_1 и μ_2. Допустим, что у нас есть биометрических 70 примеров, и мы знаем, что распределение нормальное с моментами μ_1=127.4, μ_2=13.6. Приведенная ошибка вычисления первого момента $\Delta\mu_1$=0,027. Функция распределения должна быть смещена влево (изменение стойкости преобразователя в сторону занижения) – μ_1=127,4±3,4. Приведенная ошибка определения второго момента с вероятностью, близкой к единице, $\Delta\mu_2$=0,21, он находится в пределах μ_2=13,6±2,9. С учетом наименее благоприятной ситуации кривая нормального закона смещается влево (рисунок 1). Из-за этого исходная расчетная стойкость биометрического механизма – $10^{16,84}$ к атакам подбора (правая кривая распределения значений рисунка 1) должна быть снижена до величины $10^{13,93}$, приведенная относительная ошибка в определении показателя стойкости не превышает 0,28. Даже малое количество примеров атаки (70 штук) при точном знании закона распределения дают вполне приемлемые результаты для практики. Это позволяет надеяться на то, что для получения соответствующих гарантий по стойкости биометрических средств к атакам подбора гораздо важнее знание закона распределения значения контролируемых параметров, чем объем тестовой выборки.

Таким образом, можно сделать следующие выводы:

1. Для тестирования высоконадежной биометрии необходимо создание реальных сбалансированных баз биометрических образов достаточно большого размера, позволяющих подтвердить гипотезу о том или ином законе распределения значений с высокой надежностью.

2. Если «знание» о законе распределения уже получено, то предварительное тестирование средств защиты может проводиться на выборках в 70-100 биометрических примеров.

3. Если «знание» о законе распределения уже получено, то полное тестирование средств биометрической защиты вполне может проводиться на выборках всего в десятки и сотни тысяч реальных биометрических образов с ошибкой показателя степени защищенности (отрицательного показателя вероятности ошибок второго рода) на уровне 0.1% и менее.

4. Если «знание» о законе распределения уже получено, то в место термина «оценка» стойкости средств биометрической защиты мы можем переходить к использованию термина «измерение» биометрической стойкости средств защиты. Классический эталон и его погрешность в обычных измерениях замещается на «знание» закона распределения значений контролируемой величины и доказанную (проверенную, аттестованную) погрешность этого «знания».

5. Основной задачей аттестации (сертификации) средств биометрической защиты по их стойкости является получение знаний о законе распределения выходных значений преобразователей биометрия/код.

ЛИТЕРАТУРА:

1. Иванов А.И., Петруненков А.А. Развитие биометрических технологий: объединение усилий и переход к этапу стандартизации. Журнал «Современные технологии безопасности» №3, 2004.
2. Проект ГОСТ Р (ТК 362, первая редакция) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005 г., ФГУП ПНИЭИ, ГНИИИ ПТЗИ ФСТЭК России.
3. Карасев А.И. Теория вероятностей и математическая статистика. М.: Статистика, 1970 – 344 С.
4. Боровиков В. STATISTICA: искусство анализа данных на компьютере. Для профессионалов – СПб.: Питер, 2001 – 656 С.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.65-66. Секция-2: Информационная безопасность сложных систем.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/017)

ОЦЕНКА ГРАНИЦ КОРРЕКТНОСТИ ГИПОТЕЗЫ НОРМАЛЬНОСТИ ЗАКОНА РАСПРЕДЕЛЕНИЯ ЗНАЧЕНИЙ ВЫХОДНЫХ СОСТОЯНИЙ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ/КОД

Малыгин А.Ю., Иванов А.И., Надеев Д.Н.

При производстве биометрических устройств изготовитель заявляет стойкость устройства или другими словами ошибку второго рода, показывающую «пропуск чужого». Цифры, приведенные в описаниях, в основном указываются для «среднестатистического пользователя». Ответить на вопрос реальной стойкости может только проведение тестирования по специальным методикам и на основе реальных баз биометрических образов. Исследования, проведенные в лаборатории тестирования биометрических устройств и технологий при ФВО ПГУ и лаборатории биометрических и нейросетевых технологий ПНИЭИ, показали, что высоконадежные биометрические устройства и базы биометрических данных, могут корректно описываться с помощью зависимого биномиального закона. При этом устройства с ошибками второго рода 10^{-12} и выше при модуле коэффициента корреляции менее 0.3 подставка равномерного закона распределения пренебрежимо мала в сравнении с составляющей идеального нормального закона распределения значений (рисунок 1).

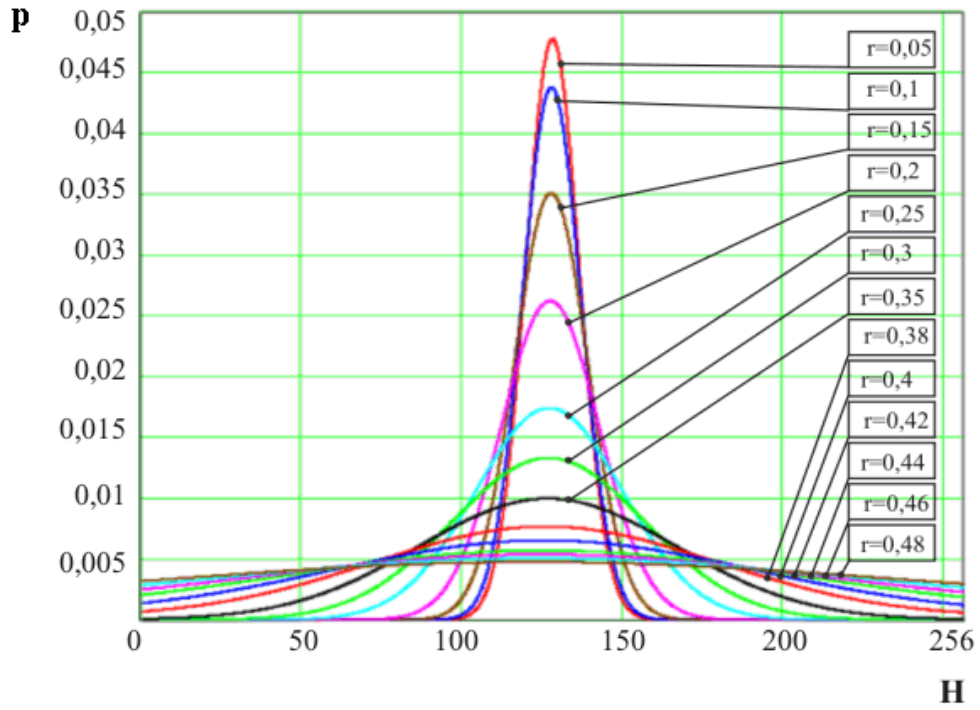

Рисунок 1 – Приближение закона распределения для зависимых данных с коэффициентом корреляции от r=0.05 до r=0.48

Относительная погрешность гипотезы нормального закона распределения (ошибка 0.05 при r = 0.3) представлена на рисунках 2 и 3, что не противоречит требованиям проекта ГОСТ Р [1].

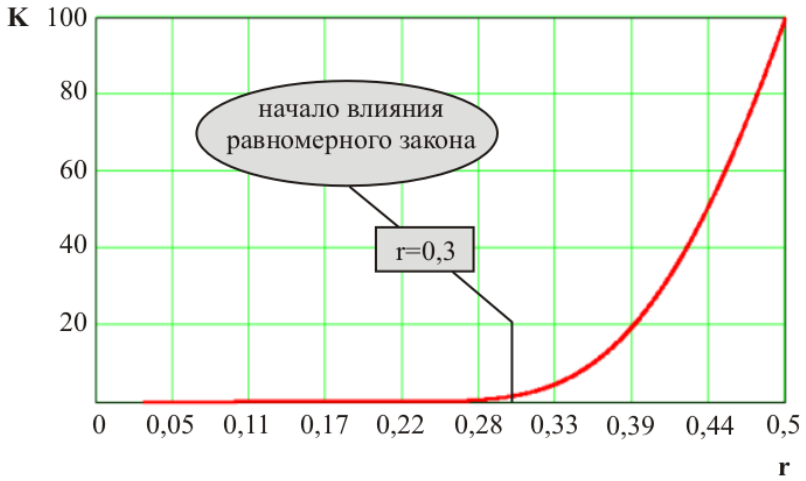

Рисунок 2 – Относительная погрешность гипотезы нормального закона распределения (ошибка 0.05 при r = 0.3)

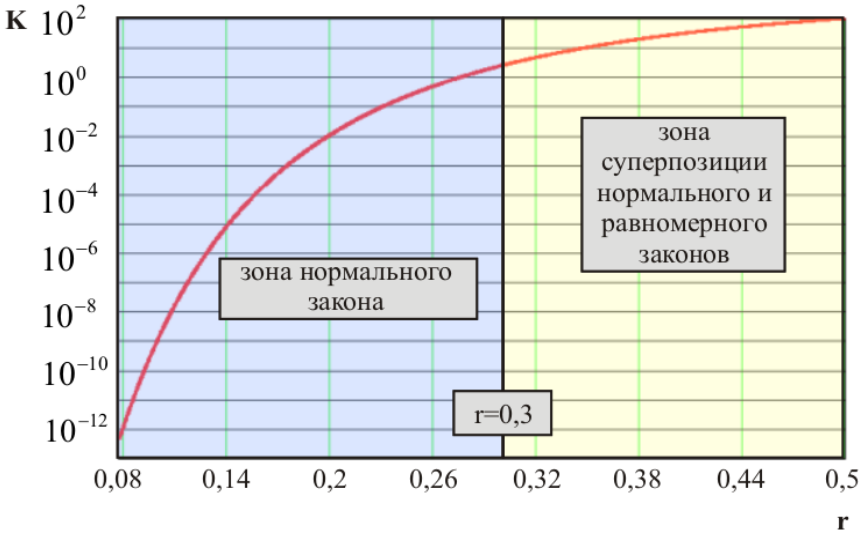

Рисунок 3 – Относительная погрешность гипотезы нормального закона распределения (логарифмическая шкала)

Получение законов распределения и зон их действия позволит тестировать биометрические устройства различной стойкости с использованием небольшого размера выборок из реальных сбалансированных биометрических баз. Это позволит сэкономить время, финансовые средства, людские и вычислительные машинные ресурсы и повысить точность тестирования реальной стойкости биометрических устройств. Наработки в этой области ставят вопрос о рассмотрении не оценок, а измерения реальной стойкости биометрических устройств.

ЛИТЕРАТУРА:

1. Проект ГОСТ Р (ТК 362, первая редакция) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005 г., ФГУП ПНИЭИ, ГНИИИ ПТЗИ ФСТЭК России.
2. Боровиков В. STATISTICA: искусство анализа данных на компьютере. Для профессионалов – СПб.: Питер, 2001 – 656 С.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.67-68. Секция-2: Информационная безопасность сложных систем.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/018)

СОПОСТАВИТЕЛЬНАЯ ОЦЕНКА СТОЙКОСТИ К АТАКАМ ПОДБОРА НЕЙРОСЕТЕВЫХ ПРЕОБРАЗОВАТЕЛЕЙ РУКОПИСНЫХ И ГОЛОСОВЫХ БИОМЕТРИЧЕСКИХ ОБРАЗОВ

Капитуров Н.В., Иванов А.И., Захаров О.С., Хозин Ю.В.

В соответствии с [1] высоконадежные средства биометрической защиты должны использовать тайные биометрические образы. Сделать тайными наиболее просто рукописные и голосовые биометрические образы. Кроме тайны на стойкость к атакам подбора влияет информативность конкретного биометрического образа. Статические биометрические образы (рисунок отпечатка пальца, рисунок вен на сетчатке глаза, рисунок радужной оболочки глаза) всегда имеют конечную информативность. Напротив, динамические биометрические образы (рукописные, голосовые) имеют неограниченную информативность, так как мы можем неограниченно увеличивать длину парольной фразы.

Очевидно, что понятие информативности того или иного биометрического образа является относительным и определяется техническими возможностями нейросетевых преобразователей. В первом приближении, нейросетевой преобразователь нечеткой, размытой биометрии в код можно рассматривать как некоторую машину обогащения сырых, бедных входных данных или биометрического информационного сырья. Эта машина исходные бедные в информационном смысле данные превращает в хорошие выходные данные (практически однозначный код ключа для образов «Свой» и случайные выходные коды, соответствующие случайным входным биометрическим образам).

Очевидно, что любая машина обогащения информации не может извлечь всю исходную информацию. Если мы возьмем более совершенную машину, то получим больший объем извлеченной информации. Оценивая потенциальную информативность того или иного биометрического образа по выходу машины обогащения, мы всегда будем иметь относительные данные, корректные только по отношению к конкретной машине обогащения информации. В этом смысле мы всегда должны оговаривать параметры машины обогащения и добычи данных.

В качестве примера рассмотрим технологию оценки информативности биометрических образов, использованную для получения таблиц А2 приложения в [1]. Для оценки информативности биометрических образов были использованы нейросетевые преобразователи рукописных и голосовых образов, имевшиеся у ФГУП «ПНИЭИ» в августе 2005 года. На конец года во ФГУП «ПНИЭИ» в действующие макеты нейросетевых преобразователей биометрия код были введены изменения, позволившие улучшить их возможности. Как следствие, необходимо скорректировать таблицу А2 во второй редакции проекта стандарта [1]. Ниже приведена скорректированная таблица потенциальной информативности рукописных и голосовых биометрических образов.

Если сравнивать голосовую и рукописную технологии защиты, то мы видим из таблицы А2, что эквивалентная длина голосового ключа примерно в 3 раза короче ключа, получаемого из такого же рукописного образа.

Таблица А.2 – Эффективные длины биометрических ключей (паролей) для среднестатистического пользователя в зависимости от числа букв биометрического пароля или от информативности тайного биометрического образа (данные ФГУП «ПНИЭИ» на декабрь 2005 года)

Число букв (цифр) в пароле, образующем биометрический образ без учета пробелов между словами	Длина ключа (пароля) получаемого из рукописного пароля (бит)	Длина ключа (пароля) полученного из голосового пароля (бит)	Длина ключа (пароля) полученного из динамических параметров клавиатурного почерка (бит)
4	32	10	-------
5	40	13	------
6	48	16	------
7	56	18	------
8	64	21	------
9	72	23	------
10	80	26	------
12	96	31	------
14	112	36	-----
16	128	42	7
18	144	47	8
20	160	52	10
24	192	64	11
26	224	76	14
32	256	88	17
36	288	100	20
40	320	112	23

Примечание 1 – В зависимости от стабильности и уникальности биометрического образа конкретного человека длина его ключа может сокращаться в три раза или увеличиваться до трех раз. Рекомендуется уточнять приведенные цифры под каждый конкретный биометрический образ через использование встроенного в биометрическое приложение механизмов тестирования и прогнозирования ожидаемой стойкости.

Примечание 2 – Для преобразователей биометрия/код эффективная длина ключа может составлять 10%,…, 30% от реальной длины выходного кода нейронной сети

ЛИТЕРАТУРА:

1. Проект ГОСТ Р (ТК 362, первая редакция) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005 г., ФГУП ПНИЭИ, ГНИИИ ПТЗИ ФСТЭК России.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.69-72. Секция-2: Информационная безопасность сложных систем.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/019)

ТРЕБОВАНИЯ К БИОМЕТРИЧЕСКИМ ВОКОДЕРАМ

Чигрин О.А., Александров Д.С., Капитуров Н.В.

Оцифровку аналогового речевого сигнала, сжатие и кодирование цифрового сигнала осуществляется с помощью вокодера. Принцип работы классических вокодеров основан на преобразовании речевого сигнала и кодирования его на небольшой скорости (1.2, 2.4, 4.8… кбит/с), позволяющей достаточно разборчиво представить любой звук в цифровой форме. Разборчивость воспроизводимых звуков ориентирована на человека и не предусматриваем последующего машинного анализа.

В параметрических вокодерах из речевого сигнала выделяют два типа параметров:

– параметры, характеризующие источник речевых колебаний (генераторную функцию) - частота основного тона, ее изменение во времени, моменты появления и исчезновения основного тона (огласованные или гортанные звуки), шумового сигнала (шипящие и свистящие звуки);

– параметры, характеризующие огибающую спектра речевого сигнала.

В декодере, соответственно, по заданным параметрам генерируются основной тон, шум, а затем пропускаются через гребенку полосовых фильтров для восстановления огибающей спектра речевого сигнала. Простейшими являются полосные вокодеры. В основе этих вокодеров лежит принцип разделения сигнала на узкие полосы в частотной области с помощью гребенки фильтров. Чем больше полос, тем качественнее восстановленный сигнал после передачи данных.

Выделяют и другие типы вокодеров:

– гомоморфные (при помощи гомоморфной обработки они позволяют разделить речевой сигнал на генераторную и фильтровую части);

– формантные (форманты - резонансные частоты голосового тракта, и в основе действия вокодера лежит их комбинация);

– ортогональные - гармонические, раскладывают речь по определенному алгоритму, в частности, ряд Фурье;

– LPC-вокодеры или липредеры используют алгоритмы линейного предсказания речи.

При разработке вокодеров ставилась задача сжатия речевого сигнала для передачи его по каналам связи и дальнейшего его восстановления на приемной части. При обычном вокодерном преобразовании многие индивидуальные характеристики голоса исчезают, так как исчезает избыточность, свойственная человеческой речи. Поэтому их применение в речевой биометрии затруднительно. На сегодня востребованы вокодеры, характеристики которых позволили бы не только обеспечивать разборчивость и высокое сжатие речи, но и применять их для последующей автоматической биометрической аутентификации.

Следует отметить, что интеллект человека во много раз превосходит искусственный интеллект современных программных и аппаратных средств. Человек может определить собеседника по первым словам: по тембру речи, интонациям, свойственным собеседнику фразам. Машинам же необходимо

множество данных для точной аутентификации. Приведем пример из смежной области – определение принадлежности рукописной подписи. Графолог понимает семантический смысл подписи, определяет её подлинность, основываясь лишь на ограниченном числе хорошо формализованных параметров, не учитывая, например, динамику написания. Машина, в свою очередь, не может понимать смысла подписи, но способна выделить сотни параметров, обработать их и на основе их анализа делать вывод о принадлежности данной подписи тому или иному человеку. На данный момент машинный анализ воспроизведения рукописных автографов на несколько порядков эффективнее экспертного анализа «мертвой подписи». Предположительно, ситуация с аутентификацией человека по голосу будет складываться сходным образом. Человек может понять семантическое содержание сказанного, но не способен обрабатывать большое число непривычных для него параметров. Машина же за счет способности выделить и обработать большое количество индивидуальных параметров при обучении, в теории должна справляться с речевой аутентификацией на несколько порядков лучше.

Поэтому в настоящее время ставится задача разработки вокодеров, которые кроме привычных функций сжатия речевой информации и перевода её в цифровой вид и обратных операций, выполняли ещё дополнительную функцию возможности использования выделенных параметров речевого сигнала для автоматической идентификации говорящего (рисунок 1).

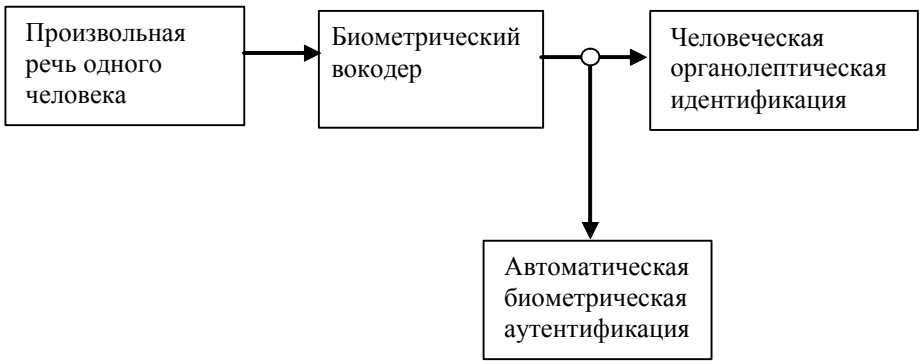

Рисунок 1 – Упрощенная схема возможной аутентификации человека с использованием биометрического вокодера

Речевой сигнал состоит из последовательности всплесков тональных колебаний, шумовых фрагментов и пауз. Каждый стационарный по энергии фрагмент в речевом сигнале соответствует некоторому фрагменту нашей речи - фонеме. Но не все фонемы одинаково эффективны при идентификации человека. Огласованные (колебательные) фонемы носят индивидуальный характер. К таким фонемам относятся звуки «э», «о», «л», «а», «и». Другая часть фонем – шипящие (шумоподобные), к ним относятся звуки «ц», «ч», «ш», «щ» и другие. Эти звуки не носят индивидуального характера, и использовать их при идентификации говорящего нельзя.[1] Одной из основных проблем является идентификация говорящего по фрагменту речи, в котором много шипящих и мало огласованных фонем. Так как выбор парольной фразы остаётся за пользователем, то данная проблема является актуальной и нуждается в решении. Современные вокодеры часто ошибаются в определении периода основного тона на коротких отдельно расположенных тональных участках речи.

Другой важной проблемой является сложность выделения тона из коротких огласованных фонем даже без определения его периода. Это так же является слабым местом у существующих вокодеров.

Речевой сигнал предоставляет информацию двух видов – о том, что сказано, и о том, кто говорит. Поэтому в речевых технологиях обычно выделяют две основные задачи – это распознавание говорящего (верификация и идентификация говорящего) и собственно разборчивое воспроизведение речи.

Выделим следующие возможности биометрико-речевых технологий: возможность скрытого распознавания говорящего в текстонезависимом режиме, документирование речи, возможность обновления говорящим своей парольной фразы при верификации в текстозависимом режиме, автоматизация проверки предъявляемого образца речи, возможность оценки психологического состояния говорящего, низкая стоимость анализа речи после его автоматизации.

Речевой сигнал существенно отличается от других сигналов своей структурной сложностью, нестабильностью параметров, избыточностью. Нестабильность параметров речевого сигнала вызвана весьма существенной вариативностью произнесения слов, что является, в свою очередь, следствием сложных явлений, происходящих в процессе речеобразования. Так, осциллограммы речевого сигнала одного и того же слова, произнесенного дважды одним говорящим, никогда не окажутся идентичными друг другу из-за различных факторов, влияющих на него в момент речеобразования. Данный факт является одновременно и проблемой, и позволяет оценить физическое и психическое состояние говорящего. Это особенно важно в ответственных приложениях, когда от действий операторов зависит жизнь или благополучие множества людей. Также биометрические вокодеры позволяют решить проблему автоматического документирования психологического состояния говорящего, то есть определения состояния автора голосовых документов. Еще одной важной проблемой, требующей решения, является распознавание содержания голосовых документов с учетом индивидуальности особенности речи.

В настоящее время просматривается три подхода к реализации биометрических вокодеров. Взаимосвязь методов реализации с учетом решаемых проблем вокодерами показана на рисунке 2. Видимо в ближайшее время должны появиться речевые вокодеры, соответствующие путям развития 2-4, 2-5, 2-6. Это связано с появлением эффективных нейросетевых биометрических приложений, соответствующих требованиям [2].

Подводя итог, можно выделить следующие основные требования к биометрическим вокодерам. Прежде всего, любой, а не только биометрический вокодер, должен обеспечивать сжатие речевой информации и при этом обеспечивать достаточную её органолептическую разборчивость. В дополнение к этим требованиям, биометрический вокодер должен обеспечивать автоматическую биометрическую аутентификацию говорящего. Часто эти требования противоречивы, и улучшение одного свойства приведет к снижению качества другого. Поэтому при разработке биометрического вокодера необходимо оптимизировать механизмы речепреобразования, возможно даже в ущерб органолептической разборчивости восстановленной речи.

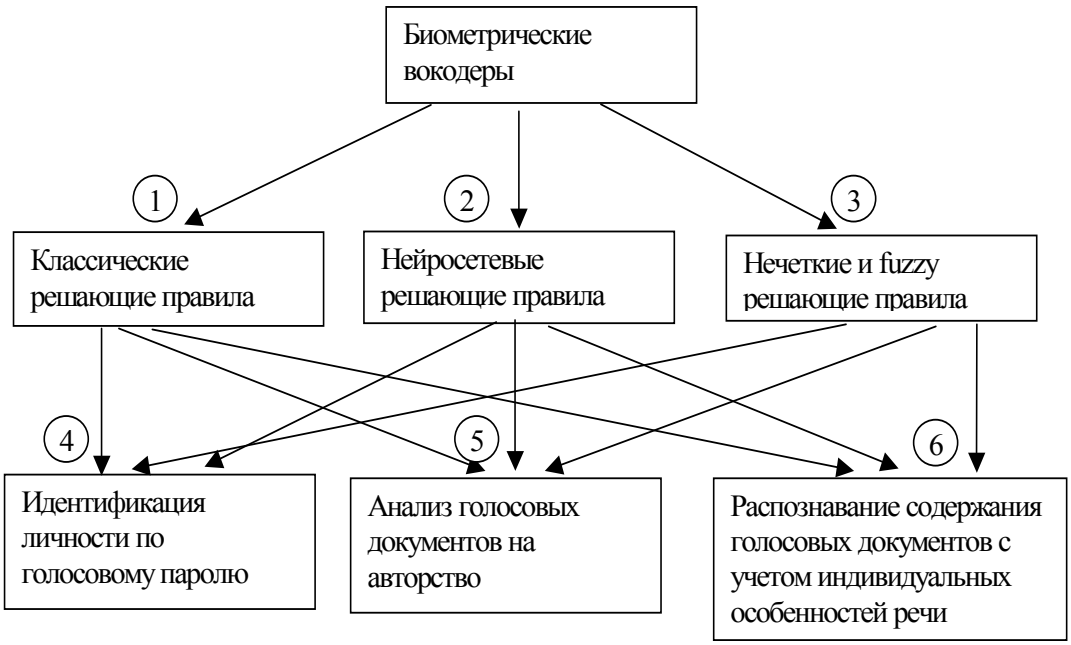

Рисунок 2 – Методы реализации биометрических вокодеров и решаемые ими проблемы

ЛИТЕРАТУРА:

1. Иванов А.И. Идентификация человека по особенностям его голоса. //Современные технологии безопасности. №3. – 2003. – с. 25-28.
2. Проект ГОСТ Р (ТК 362, первая редакция) «Защита информации. Техника защиты информации. Требования к высоконадежным биометрическим средствам аутентификации» Пенза-Воронеж-2005 г., ФГУП ПНИЭИ, ГНИИИ ПТЗИ ФСТЭК России.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.73-78. Секция-4: Анализ среды безопасности, верификация, сертификация программ.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/020)

ПРИМЕНЕНИЕ МЕТОДОВ ПОТОКОВОГО АНАЛИЗА ДЛЯ ВЫДЕЛЕНИЯ ИЗ ИСПОЛНЯЕМОГО КОДА ПРОГРАММ ИНФОРМАЦИИ О ЕЕ СТРУКТУРЕ

Соколов Е.В.
НПФ «Кристалл»

Одним из способов контроля качества программного обеспечения (ПО) является верификация. Она является одним из этапов сертификации ПО для применения в банковской, медицинской или военной сфере и представляет собой исследование программы специальными экспертами. Верификация позволяет сделать достаточно уверенные выводы относительно соответствия ПО алгоритму и отсутствия в нем различных ошибок и недокументированных возможностей. В настоящее время значительная часть работ по верификации выполняется вручную. Автоматизация процесса верификации позволила бы значительно уменьшить стоимость разработки и сертификации ПО. Кроме того, на сертификацию часто предоставляется ПО в комплектации конечного пользователя: дистрибутивный диск с исполняемыми модулями, конфигурационными файлами и эксплуатационная документация, такая как: руководство пользователя, администратора. Исходные тексты такого ПО, написанные на языке высокого уровня, обычно недоступны для специалистов по сертификации. Поэтому возникает необходимость анализа предоставленного на сертификацию исполняемого кода и извлечения из него эквивалентных ему читаемых текстов программ.

Анализ исполняемого кода проводится в несколько этапов. На первом этапе выполняется разбор заголовков двоичного исполняемого модуля и его дизассемблирование. Анализ заголовков исполняемого модуля и извлечение из них информации о секциях кода, инициализированных или неинициализированных данных представляет собой тривиальную задачу. Единственная особенность заключается в том, что инструментарий должен быть оснащен модулями разбора заголовков для всех известных форматов исполняемых модулей. Для ОС *Windows* это *DOS EXE*, *Win*16 *EXE* (*NE*), *VxD* (*LE*), *Win*32 (*PE*). Для ОС *Linux – a.out* и *ELF*.

Второй этап анализа – дизассемблирование кода. Под дизассемблированием понимается восстановление ассемблерного текста программы по ее исполняемому (двоичному) коду.

В состав любого дизассемблера обычно входит (см. рисунок 1)

– разборщик формата исполняемого файла, который выделяет из заголовка исполняемого модуля размер и положение секций кода, точек входа, данные о виртуальной памяти и другую информацию;

– управляющую часть, которая определяет адрес очередной ассемблерной команды, которая будет распознаваться;

– конечные автоматы-распознаватели отдельных ассемблерных команд, которые извлекают из памяти по адресу последовательность байт, выделяют из нее одну ассемблерную команду и вычисляют ее размер.

Для дизассемблирования одной команды управляющая часть вызывает подпрограмму, реализующую набор конечных автоматов, выполняющих

распознавание кода одной ассемблерной команды и ее параметров. Алгоритм работы этой подпрограммы очень сильно зависит от системы команд процессора, для которого написана дизассемблируемая программа. В общем случае, чем сложнее архитектура процессора, тем сложнее данная компонента дизассемблера. Запрос на дизассемблирование одной команды, как правило, содержит адрес в памяти, откуда начинается машинный код команды, виртуальный адрес в памяти, где этот код находится, когда программа загружена. Возвращаемыми значениями являются строка – текст ассемблерной команды с параметрами и размер машинной команды в памяти (если архитектура процессора допускает машинные команды переменной длины).

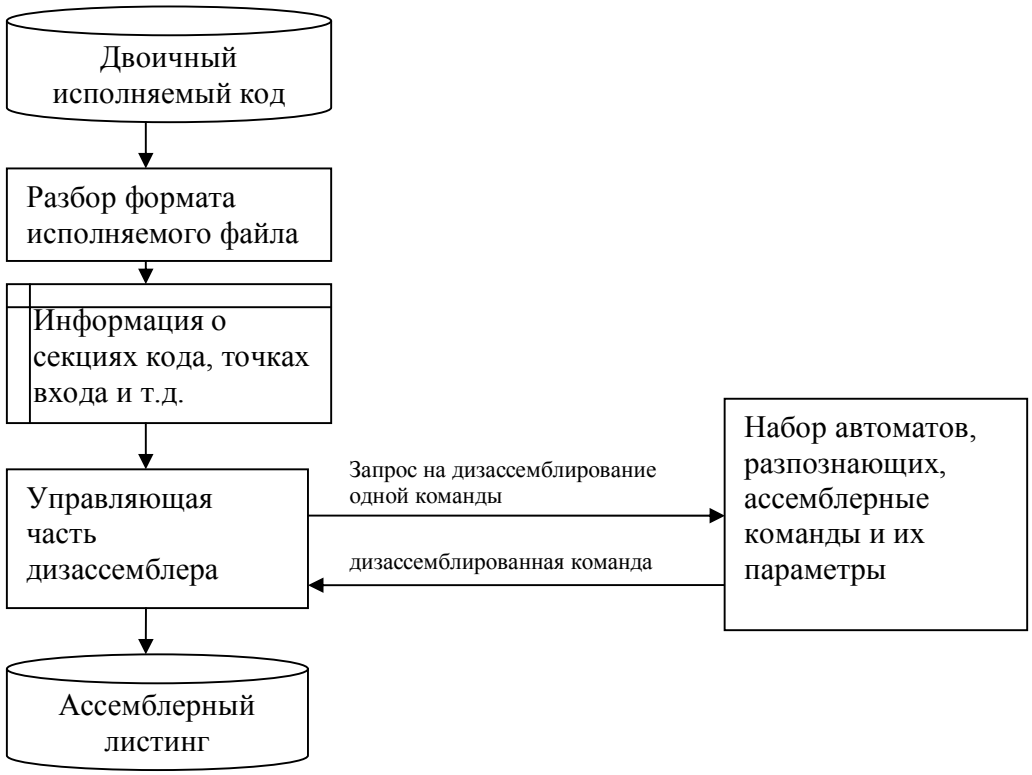

Рисунок 1 – Структура классического дизассемблера

Самые простые дизассемблеры разбирают заголовки исполняемого модуля, затем находят секцию кода и выполняют ее дизассемблирование от начала до конца. Как правило, такой подход дает неверные результаты из-за того, что в коде возможны промежутки, куда управление не попадает. Такие промежутки могут использоваться, например, для хранения данных. Однако неинтеллектуальный дизассемблер воспринимает их как ассемблерные команды. Так как размер таких промежутков может быть любым, и промежутки могут быть заполнены любым содержимым, то те ассемблерные команды, которые идут после промежутка вероятнее всего, будут распознаны неправильно и такой ассемблерный код совершенно не пригоден для автоматизированного анализа. Поэтому в технологии автоматизированного анализа необходимо применять интеллектуальное дизассемблирование от точки входа.

Принцип дизассемблирования от точки входа заключается в том, что дизассемблер ведет список точек входа в подпрограммы, куда первоначально помещается точка входа в программу. Затем из списка точек входа извлекается очередная точка входа в подпрограмму и выполняется ее последовательное дизассемблирование.

Если в процессе дизассемблирования встречается команда вызова процедуры *call*, то все возможные значения ее аргумента помещаются в список точек входа подпрограмм.

Если встречается команда безусловного или условного перехода, то все возможные значения аргумента команды помещаются в список ветвей алгоритма.

В случае безусловного перехода или команды возврата из подпрограммы *ret* обработка текущей ветви прекращается и осуществляется переход к следующей ветви.

Если ветви алгоритма текущей подпрограммы кончились, то по тому же принципу дизассемблируются все подпрограммы из списка. Критерий окончания разбора – пустой список точек входа в подпрограммы.

Список структурных единиц – процедур и функций получается непосредственно в процессе выполнения алгоритма дизассемблирования от точки входа.

Однако применение этого метода к исполняемому модулю для процессора *Intel* затруднено, т.к. команды переходов и вызовов подпрограмм могут содержать в качестве аргумента не только числовое константное значение адреса, но и регистр, адрес, хранящийся в ячейке памяти (всего 9 видов адресации), и на момент дизассемблирования команды должна быть доступна информация обо всех возможных значениях аргумента команды.

Кроме этого, есть еще одна особенность применения этого метода для программ с графическим интерфейсом. Она связна с использованием в таких программах функций «обратного вызова» (*callback*-функции). Если программисту необходимо получить уведомление от ОС о каком-либо событии (например, нажатии кнопки в диалоге), программист создает функцию реакции на это событие и указывает адрес этой функции в системном вызове. ОС при наступлении этого события вызывает функцию реакции.

Проблема функций обратного вызова может быть решена путем перечисления всех функций *API Windows*, которые принимают в качестве параметров указатель на *callback*-функцию. Это *DialogBoxParam* (макрос *DialogBox*), *CreateTimer*, *CreateThread*, *RegNotifyChangeKeyValue* и др.

Проблема определения всех возможных значений аргументов команд переходов и вызовов процедур (что необходимо для полного и корректного дизассемблирования) может быть решена методами потокового анализа.

Потоковый анализ является средством получения достоверной информации в поведении программы без ее реального исполнения. Извлекаемые из текста программы свойства – это глобальная информация о программе, которая не может быть получена ни пробными запусками программы, ни изучением ее отдельных фрагментов.

Алгоритмы потокового анализа воспринимают программу (процедуру, модуль, программную систему и т. д.) в качестве входных данных, выявляют статическую информацию (вид которой зависит от конкретной решаемой проблемы) и возвращают полученную информацию в качестве результата.

Потоковый анализ традиционно делится на два вида – анализ потока управления и анализ потока данных.

Для определения множества возможных значений аргументов управляющих команд процессора применяются методы, относящиеся к межпроцедурному анализу потоков данных. Дополнительно эти методы позволяют выявить состав параметров и возвращаемых значений процедур, входящих в модуль, а также адреса (и частично типы) локальных и глобальных переменных.

В рамках анализа потока данных необходимо построение графа связи по данным (*def-use graph*). Данный граф позволяет отследить потоки данных в программе без учета того, как именно эти данные преобразуются. Множества входов и выходов соответствуют интуитивному представлению об аргументах и результатах операторов, а отображение *Def-use* просто описывает, как используются выработанные операторами результаты. Построение данного графа опирается на решение одной из задач из области анализа потоков данных, а именно – задачи о достижимых определениях. Эту задачу можно сформулировать следующим образом: Для каждого вхождения переменной требуется определить множество присваиваний, такое, что для каждого из них существует путь, в котором между ним и данным вхождением отсутствуют другие присваивания той же переменной.

То есть задача достижимых определений заключается в выяснении, где именно устанавливаются значения того или иного вхождения данной переменной.

В связи с тем, что задача построения графа *def-use* решается для низкоуровневого ассемблерного кода, в котором все локальные переменные расположены в стеке и обращения к ним выполняются путем косвенной регистровой адресации, то возникает задача определения доступа к одним и тем же данным разными путями. Для решения этой задачи необходимо вычислять множество возможных значений для всех регистров, которые используются в качестве адресов операндов. При этом определяется, указывает адрес на сегмент инициализированных или неинициализированных данных, стековую область памяти или область памяти вне модуля и определяется, может ли операция записи по указателю инициализировать переменную, доступ к которой производится путем разыменования указателя.

После построения графа достижимых определений можно сделать выводы о данных, передаваемых в подпрограмму и обратно. Данные, передаваемые в подпрограмму (параметры) можно выявить, анализируя связи графа *def-use*, выходящие за пределы процедуры.

Параметры в подпрограмму могут передаваться несколькими способами:

1) через стек. При этом перед вызовом подпрограммы находится серия команд push или модификация указателя стека. Внутри подпрограммы, как правило, выполняется последовательность команд *push ebp*; *mov ebp esp*; *sub esp* <размер локальных переменных подпрограммы>. В результате оптимизации последовательность может не присутствовать в коде в явном виде, но семантика операций сохраняется;

2) через регистры общего назначения процессора (так называемые *fastcall*-подпрограммы). Первые два параметра таких подпрограмм передаются через регистры *eax* и *ebx*. Если у подпрограммы больше двух параметров, то они передаются через стек;

3) через глобальные (статические) переменные. Такие переменные выделяются, как правило, в сегментах (секциях) инициализированных или неинициализированных данных исполняемого модуля.

Возвращаемые значения подпрограмм (в отличие от параметров) выявляются анализом графа *def-use* не в вызываемой подпрограмме, а в одной или нескольких вызывающих. Они также могут передаваться несколькими способами:

1) единственное возвращаемое значение передается через регистр *eax*. Такой метод передачи подходит для значений, размер которых не превышает четырех байт. Более крупные возвращаемые значения передаются другими способами;

2) по указателю, переданному как параметр подпрограммы;

3) через глобальные или статические переменные.

При этом в своем поведении в отношении стека параметров подпрограммы делятся на два класса: подпрограмма сама очищает стек, содержащий параметры подпрограммы или предоставляет это делать вызывающей подпрограмме. С точки зрения выделения типов и значений параметров и возвращаемых значений эта информация не важна, но она важна для контроля за стеком.

Методы определения множества возможных значений переменных – метод разметки, метод предикат. Метод разметки заключается в том, что к каждому изменению значения переменной и каждой ветви алгоритма добавляется набор утверждений, характеризующий данную переменную или участок программы.

Для переменных, являющихся параметрами команд передачи управления набор таких утверждений на момент вызова команды передачи управления должен приводится к виду: переменная = значение1 или переменная = значение2 или … переменная = значение *N*, причем количество значений должно быть в разумных пределах.

Поскольку конечной целью анализа является получение псевдокода исследуемой программы на языке программирования высокого уровня, то целесообразно объединить управляющую часть дизассемблера и программные компоненты, выполняющие потоковый анализ в один программный модуль – дизассемблер автоматизированного анализа. Структура такого дизассемблера представлена на рисунке 2.

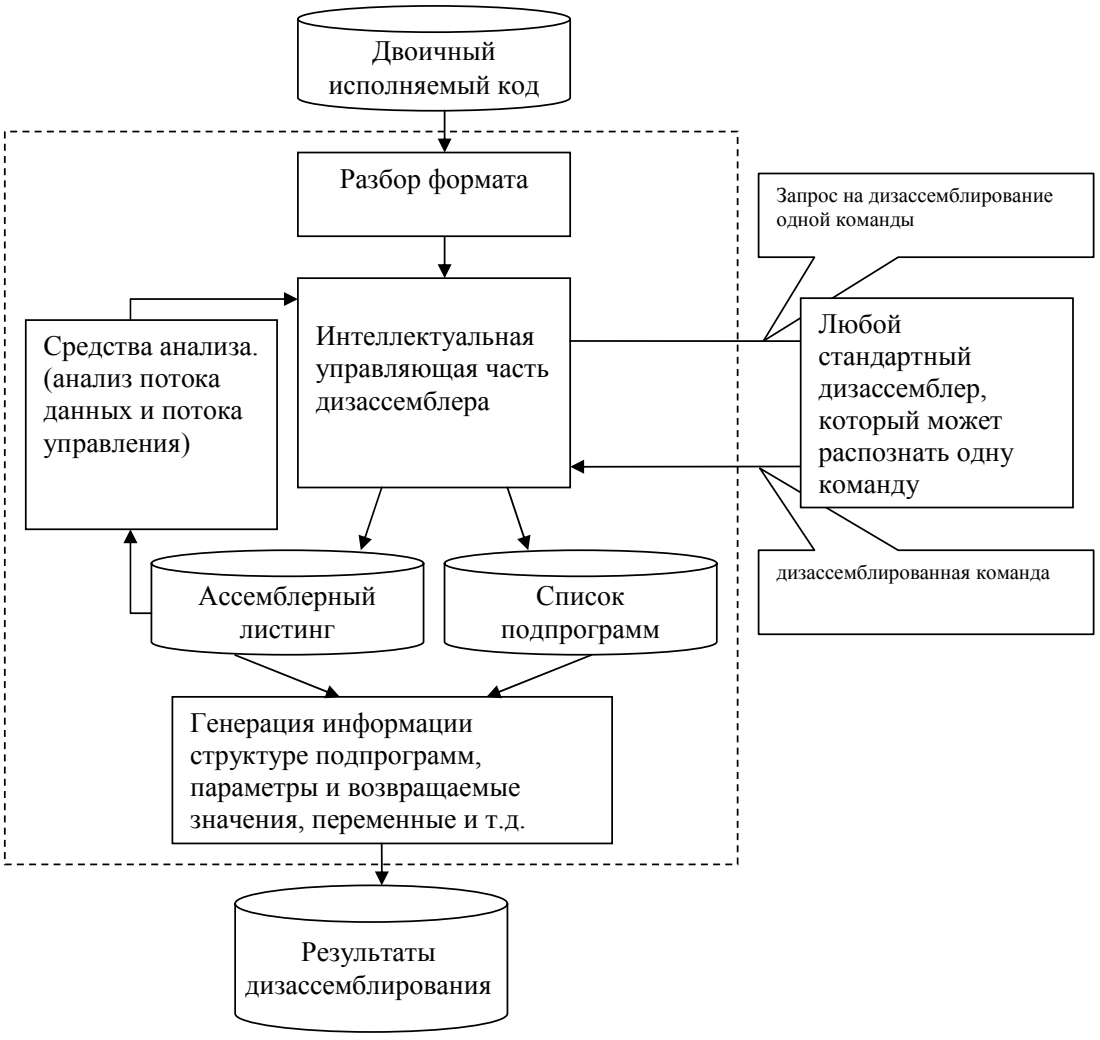

Рисунок 2 – Структура дизассемблера автоматизированного анализа

Алгоритм дизассемблирования от точки входа, реализованный в ДАА, выглядит следующим образом.

Создается список ветвей алгоритма. Каждый элемент такого списка в отличие от классического метода является не адресом-константой, а переменной, которая может содержать, константу, ссылку на регистр, ссылку на ячейку памяти, и выражение, содержащее все вышеперечисленные элементы, а также операции обращения по адресу, сложения и умножения.

При дизассемблировании очередной ветви алгоритма происходит занесение в список ветвей алгоритма переменных – аргументов команд передачи управления и вызовов процедур. На первом этапе вычисляется одно из возможных значений переменной, соответствующее прямому выполнению ветви от начала процедуры. По мере дизассемблирования новых ветвей и новых процедур выполняется частичный анализ потока данных программы и строится разметка программы для переменных – аргументов команд передачи управления, а также данных, которых зависят эти переменные. В результате разметки переменные приобретают новые возможные значения, соответствующие новым ветвям алгоритма или новым процедурам. Эти ветви и процедуры также должны быть дизассемблированы.

Таким образом, управляющая часть реализует итерационный алгоритм, состоящий из этапов «дизассемблирование» → «выявление переменных-аргументов команд передачи управление» → «разметка дизассемблированной части программы по этим переменным» → «выявление множества возможных значений» → «добавление новых ветвей алгоритма или процедур» → «дизассемблирование……». Критерием окончания работы алгоритма является прекращение появления новых ветвей алгоритма или процедур на очередной итерации.

ЛИТЕРАТУРА:

1. Бродин В.Б. Шагурин И.И. Микропроцессор i486. Архитектура, программирование, интерфейс. – М.: Диалог-мифи, 1993.
2. Касьянов В.Н. Оптимизирующие преобразования программ, М., "Наука", 1988. 336 с.
3. Касперски К. Образ мышления-дизассемблер IDA. Том 1 – М.: СОЛОН – Р, 2001.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.79-100. Секция-3: Нормативное, методологическое и методическое обеспечение информационной безопасности.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/021)

ОБЕСПЕЧЕНИЕ И ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СИСТЕМ. ТЕКУЩИЙ МОМЕНТ И ПЕРСПЕКТИВЫ

Голованов В.Б.
ООО НПФ «Кристалл»

Несмотря на значительные усилия, вкладываемые в развитие технологий, методов и средств обеспечения информационной безопасности (ИБ) организаций и их систем информационных технологий и автоматизированных систем, к настоящему времени острота вопроса не спадает, а в большинстве случаев даже увеличивается. В этой связи представляет определенный интерес рассмотреть текущий момент в его некоторой исторической ретроспективе, позволяющей понять аспекты эволюции вопроса, с точки зрения потенциального владельца или пользователя систем информационных технологий и автоматизированных систем и в контексте потенциальной практической отдачи от предлагаемых зарубежных или отечественных решений.

Революционная эволюция

Широкое распространение информационных технологий (ИТ) в современном обществе, расширение круга числа их пользователей привело к увеличению потребности в обеспечении ИБ с одновременным ростом интереса к этой области техники. Современный мир немыслим без компьютеров и средств коммуникаций, что осознано и поддерживается, в том числе, и на государственном уровне, как в нормативном плане, так и в практическом в форме различных Федеральных целевых программ, таких как «Электронная Россия» и т.п. В этой связи определенный интерес представляют анализ и оценка того, а что же может на сегодняшний день предложить индустрия (отрасль) ИБ для пользователей и владельцев систем ИТ и автоматизированных систем (АС)[2)], пользователей и владельцев информации[3)].

Конец 90-х годов прошлого века и начало 2000-х как в международном сообществе, так и в России прошел под флагом коренной ломки сложившихся в середине 80-х годов подходов к защите информации, направленной на защиту от несанкционированного доступа (НСД). Флагманом нового подхода, новой технологии на конец 90-х годов стал принятый ИСО в 1999 году международный стандарт ISO/IEC 15408:1999 [1], который на международном уровне закрепил технологию, более известную как «Общие критерии».

Примерно в эти же годы в России инициировался процесс по гармонизации в стране новой технологии, отраженной в международном стандарте ISO/IEC 15408:1999, для целей замены ею требований Руководящих документов (РД) Гостехкомиссии при Президенте Российской Федерации [2÷7]. РД Гостехкомиссии от 1992 года, в свою очередь, представляли аналог требований американской серии документов от 1985 года, более известной под названием «Оранжевая книга». Это был большой шаг вперед и на тот период многим

[2)] Под системами ИТ здесь понимается комплекс средств автоматизации в составе АС.

[3)] Обладателей информации – в терминах проекта новой редакции Федерального закона «Об информации, информационных технологиях и защите информации».

специалистам подход ISO/IEC 15408:1999 виделся некоей панацеей – рецептом решения проблем на все случаи жизни, который должен был позволить обеспечить решение задач безопасности ИТ, информационной безопасности и защиты информации как на уровне отдельных продуктов ИТ, так и на уровне систем ИТ, а в перспективе и АС. Одновременно многие организации, такие как Банк России, Центр безопасности информации, Центр «Атомзащитаинформ», ЦНИИАтоминформ провели достаточно глубокие как самостоятельные (Банк России), так и по заказу (Гостехкомиссии при Президенте Российской Федерации) исследования по возможности использования стандарта ISO/IEC 15408:1999 как корпоративных, так и в общенациональных интересах. Материалы нового международного стандарта, а также направления его практического применения были рассмотрены в ряде книг и публикаций [8÷11]. В итоге в апреле 2002 года был принят российский аналог ISO/IEC 15408:1999 – ГОСТ Р ИСО/МЭК 15408-2002 с датой введения его в действие через полтора года – с 1 января 2004 года.

Мифы относительно того, что стандарт ISO/IEC 15408:1999 позволит решить все проблемы разработчиков, оценщиков и пользователей оцененной продукции в части использования единого и понятного участникам языка общения, развеялись при первых попытках практической реализации. Такие результаты были в основном обусловлены тем, что стандарт ISO/IEC 15408:1999, и это, в общем-то, не секрет для специалистов, был ориентирован под нужды рынка средств безопасности ИТ, и его спонсорами выступали ведущие мировые производители средств (самостоятельных продуктов) информационной безопасности. Поэтому все попытки применения стандарта для решения задач обеспечения безопасности на уровне систем ИТ, а тем более АС, заканчивались безуспешно. При ближайшем рассмотрении выявлялась, что называется, «системная несовместимость», что, в общем-то, и неудивительно.

Примерно в тоже время, что и стандарт ISO/IEC 15408:1999 в ИСО по ускоренной процедуре, которая заняла всего полгода, был принят другой международный стандарт ISO/IEC 17799:2000 [12]. Международный стандарт ISO/IEC 17799:2000 в отличие от ISO/IEC 15408:1999 более ориентирован на потребности организации в целом, нежели только в части ИТ, и включает рассмотрение таких аспектов, как организационные вопросы безопасности, политика безопасности организации, физическая защита, безопасность взаимодействия и коммуникаций и пр. Данный международный стандарт, как отмечалось, был принят по ускоренной и упрощенной процедуре, предусмотренной для принятия существующих национальных и иных стандартов, положительно зарекомендовавших себя на международном уровне. Прототипом ISO/IEC 17799:2000 послужила первая часть британского стандарта BS 7799, содержавшего свод правил (практик) менеджмента информационной безопасности.

К концу 90-х годов прошлого века сложилась ситуация, когда ведущую роль в обеспечении информационной безопасности заняли оба международных стандарта: ISO/IEC 15408:1999 и ISO/IEC 17799:2000 (с учетом BS 7799-2 [13]). При этом многие пользователи данных документов использовали те или иные их части, определенным образом решая вопросы по их взаимной увязке. Практически такая же ситуация сложилась и в международном сообществе, что вынудило и послужило поводом для принятия соответствующих решений и мер, позволяющих выработать единые подходы при использовании данных документов.

Сближение двух подходов

Основные цели, направления и пути сближения стандартов ISO/IEC 15408:1999 и ISO/IEC 17799:2000 (с учетом BS 7799-2 [13]) рассмотрены в [14]. Приведем здесь основные различия и, следовательно, направления, требующие рассмотрения для сближения указанных стандартов.

К первому принципиальному отличию следует отнести разное понимание, вкладываемое в понятие «сертификации» и связанный с этим вопрос о воспроизводимости результатов сертификации.

Сертификация по ISO/IEC 15408:1999 действительна только на ту дату, когда оценщики представляют свои результаты. Хотя компоненты Общей методологии оценки и требований доверия к безопасности существуют для поддержки действительности сертификата, их использование не обязательно и зависит от предположения, что результаты сертификации могут быть недействительными только в результате изменений в объекте оценки (ОО).

Сертификация же по BS 7799 требует наличия в организации системы менеджмента[4)] информационной безопасности (СМИБ), которая ведет мониторинг того, насколько эффективно продолжают работать средства управления безопасностью и после даты оценки и/или сертификации и т.д. Сертификация по BS 7799 означает уверенность, что СМИБ должна функционировать эффективно до даты следующей проверки СМИБ в рамках надзорной аудиторской деятельности органа сертификации.

К другому принципиальному отличию следует отнести определения понятия, которое вкладывается в термин «система».

Система в ISO/IEC 15408:1999 определяется как специальная инсталляция ИТ с определенной целью и в определенной среде. В ISO/IEC 17799:2000 и BS 7799-2 этот термин понимается в более широком смысле бизнеса вообще, включая его организацию, место расположения, активы и технологию. Отсюда вытекают определенные последствия, в частности, в отношении к среде в ISO/IEC 15408:1999, которая рассматривается менее динамичной и менее подверженной изменениям.

К третьему отличию можно отнести распределение ролей безопасности.

Ответственность за безопасность по ISO/IEC 17799:2000 (BS 7799-2) возлагается на организацию, владеющую системой. В ISO/IEC 15408:1999 она возлагается на разработчика системы. В свою очередь, это отражает основное предположение ISO/IEC 15408:1999, что система, которая оценивается, является обычно новой, построенной, тогда как в BS 7799-2 предполагается, что система, подлежащая сертификации по безопасности, уже эксплуатируется.

Четвертое отличие порождается отношением к «менеджменту безопасности».

Менеджмент безопасности в ISO/IEC 17799:2000 и BS 7799-2 означает процесс, являющийся частью общей системы менеджмента организации, предназначенной для управления рисками бизнеса. В ISO/IEC 15408:1999 менеджмент безопасности – это административный процесс, предназначенный для обеспечения безопасности установки и работы системы ИТ.

В соответствии с принципиально разным подходом к менеджменту безопасности, принципиально по-разному формируется отношение к понятию «риск».

Риск в ISO/IEC 17799:2000 и BS 7799-2 предполагается непрерывно изменяющимся во времени по причине изменений в организации, технологии,

---

[4)] Понятие «менеджмент» определено, например, в ГОСТ Р ИСО 9000 как: скоординированная деятельность по руководству и управлению организацией.

угрозах и т. д. В ISO/IEC 15408:1999 риск предполагается статическим до возникновения системных изменений или новых угроз/уязвимостей.

В связи с этим, в рассматриваемых стандартах по-разному понимаются и «цели безопасности» и «цели управления».

Цели безопасности и *цели управления* рассматриваются в ISO/IEC 17799:2000 и BS 7799-2 неразрывно. Использование (ограниченное) термина «цель безопасности» идентично с ISO/IEC 15408:1999. Термин «цель управления» используется для группы средств управления, связанных общим типом рисков, которые они снижают или исключают. В принципе, средства управления безопасностью в ISO/IEC 17799:2000 и цели безопасности в ISO/IEC 15408:1999 представляют одно и тоже понятие, хотя они выражены несколько по-разному.

Всем, кто заинтересован и внимательно отслеживает, изучает или делает попытки внедрения рассматриваемых стандартов, отмеченные различия известны.

Данные различия неоднократно обсуждались как в рамках международного сообщества, например, в рамках 27 подкомитета (SC27) «Методы и средства безопасности» первого совместного технического комитета ИСО и МЭК «Информационные технологии», так и в нашей стране. Конкретное направление решения этого вопроса было определено на совещании третьей рабочей группы (WG3) SC27 (разработчика международного стандарта ISO/IEC 15408:1999), состоявшегося в октябре 2002 года в Варшаве. Временная рабочая группа по изучению проблемы оценки систем в составе WG3, возглавляемая японскими экспертами, запросила от ассоциации «BS 7799 World» разработку, показывающую как BS 7799-2 и ISO/IEC 17799 могут использоваться в качестве критериев и методологии для оценки частей действующих систем, не относящихся к ИТ.

По данному поручению была проведена соответствующая работа, что зафиксировано в 607-ом документе WG3 [15]. В решении WG3 отмечалась необходимость развития оценки действующих систем в направлении расширения сферы оценки, включающей все цели безопасности системы, а не только стандартные цели объекта оценки[5)] по требованиям ISO/IEC 15408:1999, включающие цели для комплекса средств автоматизации АС. Развитие подходов ISO/IEC 15408:1999 было предложено ориентировать на использование существующих стандартов ISO/IEC 17799:2000 и BS 7799 при определении не ИТ-целей и требований безопасности.

В принципе это и послужило идеологической основой нового документа ИСО, который получил номер 19791 и общее название проекта «Оценка безопасности эксплуатирующихся систем» («*Security assessment of operational systems*»).

Поиск подходов к оценке безопасности систем

Проект ИСО 19791 «Оценка безопасности эксплуатирующихся систем» был заявлен как расширение к международному стандарту ISO/IEC 15408 в части рассмотрения тех аспектов среды эксплуатирующихся систем, которые не рассматриваются требованиями и моделями ISO/IEC 15408. Основные расширения заявлены как предназначенные для оценки среды эксплуатации объекта оценки – системы, а также для декомпозиции сложных эксплуатирующихся систем на домены безопасности, которые далее можно было

[5)] Понятие «объект оценки» по ГОСТ Р ИСО/МЭК 15408 определяется как: подлежащий оценке продукт информационной технологии или система с руководствами администратора и пользователя.

бы оценить каждый в отдельности. Оценка эксплуатирующихся систем, как отмечается в тексте ISO/IEC TR 19791, нацелена на обеспечение условий их последующей сертификации и аттестации. В то же время, положения документа ISO/IEC 19791 не раскрывают такие вопросы, как:

– цели сертификации и аттестации систем и того, что (какие гарантии и кто) дает такая сертификация для владельца системы;

– требования к органам аттестации, сертификации и оценки;

– соответствующие правила, процедуру и методики, включая использование сертификатов.

В апреле 2002 года был опубликован первый информационный технический отчет о результатах деятельности рабочей группы по поиску подходов к оценке безопасности эксплуатирующихся систем [16]. Материалы данного отчета касаются вопросов применения ISO/IEC 15408 для систем ИТ, эксплуатируемых в организациях, и содержат следующие основные положения. Представлен типовой состав систем ИТ с точки зрения возможностей и целей оценки. На рисунке 1 представлены три типа компонентов системы, как это сделано в отчете рабочей группы.

Прикладные системные программы
Прикладная программа включает в себя бизнес-программы и эксплуатационные программы, предназначенные для конкретной системы. Компоненты данного уровня могут быть доступны для оценки.
Покупные продукты ИТ (операционные системы, системы управления базами данных, почтовые приложения и т. п.)
Внешние интерфейсы продуктов ИТ, если они являются внешними для системы, доступны для оценки. Интерфейсы между продуктами и внутренние интерфейсы каждого продукта не всегда доступны для оценки. Не все продукты всегда оцениваются.
Аппаратные средства (процессоры, устройства ввода/вывода и т. п.)
Как правило, аппаратные средства имеют непосредственные интерфейсы только с операционными системами.

Рисунок 1 - Типовая структура системы и возможности оценки

Поскольку система всегда состоит из частей, степень структурированности частей системы должна всегда приниматься в расчет при решении о том, какие действия по анализу требуются от оценщика во время оценки системы.

Далее в техническом отчете рассмотрены вопросы, касающиеся среды разработки и среды эксплуатации систем ИТ. Обозначены основные подходы по разработке и введению пакетов доверия для оценки систем, рассмотрены отличия требований для управления безопасностью систем.

В контексте требований к управлению системами авторы технического отчета обратили внимание на то, что эти требования должны включать требования для управления контрмерами безопасности применительно к операциям персонала и пользователей, физическим ошибкам, природным бедствиям и т.д. Для этих целей было предложено использовать практики безопасности из международного стандарта ISO/IEC 17799:2000. При этом отмечалось, что контрмеры управления могут быть определены как цели

безопасности так, чтобы требования к управлению могли бы быть использованы как некое дополнительное множество требований для систем ИТ в дополнение к функциональным требованиям и требованиям доверия из ISO/IEC 15408.

Наряду с указанным, была предложена классификация и структуризация требований стандарта ISO/IEC 17799:2000 подобная той, которая представлена в частях 2 и 3 ISO/IEC 15408, а именно – класс, семейство, компонент требований. Содержание классов требований предложено отобразить на структуру разделов стандарта ISO/IEC 17799:2000, семейства классов – на подразделы, а все последующие уровни иерархии материалов стандарта ISO/IEC 17799:2000 отобразить в виде элементарных компонентов требований. Также предложена уникальная идентификация требований по управлению из ISO/IEC 17799:2000 подобная той, которая применена в ISO/IEC 15408. В одном из приложений к техническому отчету [16] приведена возможная структура каталога требований по управлению информационной безопасностью, разработанная на основе стандарта ИСО/МЭК 17799.

Дальнейшее развитие деятельности рабочей группы SC27 по вопросам, связанным со спецификой оценки систем нашло отражение во втором «Оценка систем. Принципы, концепции, термины» [17] и третьем «Оценка безопасности эксплуатирующихся систем» [18] информационных отчетах рабочей группы, которые были опубликованы в октябре 2002 г. и апреле 2003 г., соответственно, и в целях обсуждения сформированных подходов распространены среди экспертов третьей рабочей группы SC27.

В результате 2-хлетней работы над документом была разработана базовая редакция документа [19], материалы которой включают изложение следующих позиций:

- суть предлагаемых решений (раздел 6 «Технический подход»), включая рассмотрение:
  - основных свойств эксплуатирующихся систем;
  - свойств безопасности эксплуатирующейся системы;
  - безопасности на жизненном цикле эксплуатирующейся системы;
  - доверия к безопасности эксплуатирующейся системы;
  - взаимодействия с другими системами;
  - композитные (сложные) эксплуатирующиеся системы;
- отношение предлагаемых решений к стандарту ISO/IEC 15408 (раздел 7 «Расширение концепций оценки ISO/IEC 15408 на эксплуатирующиеся системы»), включая:
  - общую философию;
  - типы средств управления безопасностью;
  - дополнительные оценочные требования;
  - время, необходимое для проведения оценки;
  - использование оцененных продуктов;
  - требования к документации;
  - процесс тестирования;
  - менеджмент конфигурации;
- отношения к другим стандартам (раздел 8 «Связь с существующими стандартами по безопасности»), включая:
  - связь с ISO/IEC 15408;
  - связь с неоценочными стандартами, под которыми в документе подразумеваются ISO/IEC 17799 и руководство НИСТ США NIST SP 800-53

«Рекомендованные средства управления безопасностью для федеральных систем»;

– непосредственно требования к оценке безопасности эксплуатирующихся систем (раздел 9 «Оценка эксплуатирующихся систем»), включая:

- роли и обязанности при оценке;
- оценка риска и определение порога приемлемого риска;
- формулировка проблемы (потребностей) в безопасности;
- цели безопасности;
- требования безопасности;
- системное задание по безопасности (СЗБ);
- периодическая переоценка;

– формальные требования к профилям защиты и заданиям по безопасности, которые введены ISO/IEC 15408, но для систем (Приложение A), включая:

- спецификацию заданий по безопасности на систему;
- спецификацию профилей защиты на систему;

– дополнительные по отношению к ISO/IEC 15408 функциональные требования безопасности, ориентированные на оценку систем (Приложение B), включая следующие классы требований:

- класс FOD: Администрирование;
- класс FOS: Системы ИТ;
- класс FOA: Пользовательские активы;
- класс FOB: Бизнес;
- класс FOP: Помещения и оборудование;
- класс FOT: Третьи стороны;
- класс FOM: Менеджмент;

– дополнительные по отношению к ISO/IEC 15408 требования обеспечения доверия безопасности (оценки), ориентированные на оценку систем (Приложение C), включая следующие классы требований:

- класс ASP: Оценка системного профиля защиты;
- класс ASS: Оценка системного задания по безопасности;
- класс AOD: Руководящая документация на эксплуатирующуюся систему;
- класс ASD: Документация по архитектуре, конструкторская документация и документация по конфигурации эксплуатирующейся системы;
- класс AOC: Менеджмент конфигурации эксплуатирующейся системы;
- класс AOT: Тест эксплуатирующейся системы;
- класс AOV: Анализ уязвимости эксплуатирующейся системы;
- класс AOL: Обеспечение жизненного цикла эксплуатирующейся системы;
- класс ASI: Поставка и установка системных средств обеспечения безопасности;
- класс ASO: Записи в эксплуатирующейся системе.

Не будем подробно останавливаться на характеристике и описании материалов, вошедших в документ – они достаточно подробно раскрыты в [20]. В то же время, учитывая значительную его новизну и имеющийся интерес к нему,

обратим внимание на основные вопросы, которые следуют из обсуждения данного документа экспертами международных организаций [21].

Так, например, поднимая вопрос согласованности проекта ISO/IEC TR 19791 с Общими критериями (ISO/IEC 15408), специалисты из немецкого национального Института стандартизации обратили внимание на то, что из данной редакции рассматриваемого проекта до сих пор нельзя однозначно понять описывает ли данный документ способ применения действующей редакции «Общих критериев» (ОК) (ISO/IEC 15408) в отношении эксплуатирующихся систем или же в нем сформулированы модифицированные ОК для них.

По мнению немецкой стороны, было бы предпочтительным первое решение: разрабатываемый технический отчет должен выступать в качестве поддерживающего документа для ОК, что и планировалось при постановке проекта, и должен описывать применение ОК в отношении эксплуатирующихся систем. Проект не должен являться еще одним вариантом ОК.

Разработчики проекта подтвердили, что разрабатывается именно руководство по применению требований безопасности к эксплуатирующимся системам, а не новый вариант ОК и дал ряд следующих пояснений.

В контексте ОК (ISO/IEC 15408) эксплуатирующаяся система также является Объектом оценки, однако присутствуют некоторые области, для оценки которых существующих требований не достаточно. Одним из примеров является оценка эксплуатационно-операционных требований безопасности (требований к операционным защитным мерам – мерам, которые выполняются людьми в отличие от систем). При этом существующие критерии ОК не позволяют рассмотреть операционные средства управления (защитные меры) с точки зрения функциональности и доверия.

В связи с этим в приложениях разрабатываемого отчета представлены дополнительные требования, необходимые для подобного рода оценок, и предложены способы расширения ОК для проведения оценки эксплуатирующихся систем.

Тем не менее, изначально, как отмечается в резолюции, не существовало никаких намерений размещать в данном техническом отчете каких бы то ни было детальных расширений для действующих ОК. Существующие функциональные требования безопасности ISO/IEC 15408, как заявлено разработчиками нового документа, но вызывает сомнения при практическом рассмотрении, в равной мере применимы для эксплуатирующихся систем без необходимости внесения каких-либо изменений, т. е. ISO/IEC TR 19791 не накладывает никаких дополнительных требований в части оценки продуктов ИТ, разработанных и оцененных по ISO/IEC 15408, при их использовании в составе эксплуатирующихся систем.

Что касается требований обеспечения доверия, появилась необходимость внесения некоторых расширений в компоненты требований доверия. В связи с этим полный перечень таких требований представлен в приложении С проекта документа (см. представленную выше структуру документа), при этом соответствующие части действующих критериев ОК приведены без изменений. Также отмечается, что при анализе действующей версии того или иного компонента требований ОК, на основании его применимости, авторы технического отчета принимали решение: переименовывать компонент или только модифицировать его элементы. Потребность в дополнительных критериях обусловлена свойствами и целями безопасности, которые не охвачены областью оценки по действующим ОК. Отмечается, что ОК и, в особенности, критерии доверия не предназначены для оценки операционных средств управления и

достаточно точная интерпретация с целью проведения подобной независимой объективной оценки по ним представляется затруднительной.

В равной степени, в проекте ISO/IEC TR 19791 не определено никаких новых критериев для оценки технических средств управления (защитных мер). Авторами использован такой подход, при котором средства управления, представленные в ОК (или ISO/IEC 15408), полностью используются для обеспечения реализации свойств и целей безопасности, лежащих в области действия существующих ОК. Авторы документа допускают и приветствуют использование сертифицированных по ISO/IEC 15408 продуктов в составе оцениваемых эксплуатирующихся систем, однако отмечают возможность появления проблем их взаимной или системной интеграции. Проблемы могут быть связаны с различиями в конфигурации оцененного продукта при его оценке и сертификации и конфигурации в реальной эксплуатационной среде, следовательно, это приводит к потере актуальности результатов его оценки. В другом случае, уровень доверия оцененного продукта может оказаться неадекватным допустимому уровню доверия при интеграции оцененных продуктов ИТ в систему. В проекте ISO/IEC TR 19791 представлены отдельные возможные направления действий для решения данных проблем.

Другим важным вопросом, поднятым немецкими экспертами являлся вопрос о методологии оценки безопасности эксплуатирующейся системы. В нем отмечается, что предыдущие версии проекта содержали некоторые части Общей методологии оценки (ОМО) по ОК или, по крайней мере, о них было заявлено в документе. Но в последней редакции упоминания о методологии отсутствуют вовсе. Этот факт, как отмечалось, вызывает определенное беспокойство по поводу возможных проблем, т. к. в отсутствие опубликованной и признанной методологии оценки для новых требований доверия для эксплуатирующихся систем данный технический отчет будет абсолютно бесполезным, как для спонсоров оценок, включая собственников эксплуатирующихся систем ИТ, так и для самих оценщиков.

Для решения данного вопроса немецкая сторона предложила включить в проект отчета соответствующую методологию оценки или, в случае, если это не планируется сделать, включить в отчет информацию о том, как оценщик может получить руководство по применению требований обеспечения доверия, определенных в приложении к отчету. Рекомендация была одобрена и так как руководство для оценщиков не попадает в поле действия рассматриваемого технического отчета, для разработки такого руководства необходимо начать новое направление работ в рамках ISO/IEC.

О чем это говорит, и что из этого следует. А следует из этого, что собственникам систем ИТ эффективно применять на практике ISO/IEC TR 19791 не представляется возможным. Согласно принятой на уровне ИСО модели оценки безопасности ИТ должны быть определены и представлены три уровня модели (см. рисунок 2).

Принятие ISO/IEC TR 19791 обеспечивает поддержку «верхнего уровня» модели оценки. В тоже время отсутствие принятой методологии не позволяет охватить все уровни модели и вносит свои особенности в возможность применения документа в практике.

Определенный интерес представляет соотнесение (сравнение) технического отчета ISO/IEC TR 19791 с другими существующими стандартами по безопасности ИТ.

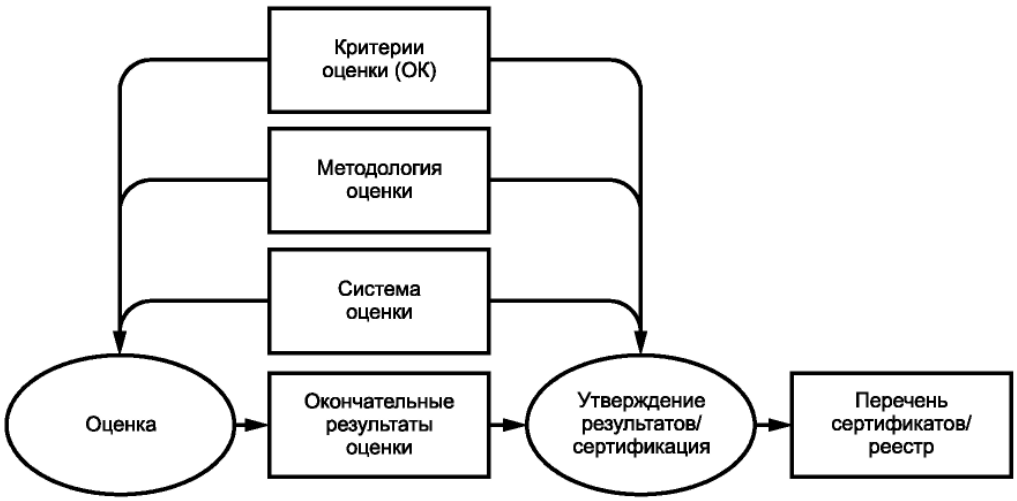

Рисунок 2 – Модель оценки

Необходимые для оценки процессы, документы и задачи (работы) в определенной части сформулированы в рассматриваемом отчете посредством расширения (дополнения) аналогичных концепций из ISO/IEC 15408. Дополнительные критерии оценки предназначены, в первую очередь, для оценки не-ИТ аспектов ИБ при интеграции и эксплуатации системы. Они получены разработчиками отчета из существующих стандартов по ИБ. В частности, текст проекта технического отчета ISO/IEC TR 19791, как и планировалось, в значительной степени основывается на двух характерных стандартах лучших практик по ИБ – ISO/IEC 17799 и руководстве НИСТ США NIST SP 800-53 «Рекомендованные средства управления безопасностью для федеральных систем». С учетом широкого распространения данных документов, авторы сочли самостоятельную разработку новых критериев и их структуры нецелесообразной, и заимствовали соответствующие положения из данных документов.

Соотношение между средой эксплуатации и критериями оценки представлено в графическом виде на рисунке 3. Системное задание по безопасности, модель политики безопасности системы, документация по оценке риска, анализу уязвимостей, руководящая документация, процедуры и проектно-конструкторская документация являются необходимыми составляющими пакета документов, предоставляемого для оценки системы. Перечень данных документов сформирован на основе требований стандарта ISO/IEC 15408.

Что касается критериев оценки среды эксплуатации, а именно оценки операционных средств управления (средств защиты), такие критерии заимствованы из стандартов и руководящих указаний ISO/IEC 17799, ISO/IEC 21827, NIST SP 800-53 и др.

Авторы отчета отмечают, что наряду с ISO/IEC 17799 и NIST SP 800-53 в качестве источников были использованы и некоторые другие стандарты SC27, такие как ISO/IEC 13335 и ISO/IEC 21827. Технический отчет ISO/IEC TR 15443 послужил источником альтернативных возможных подходов в отношении требований доверия, а технический отчет ISO/IEC TR 15446 – источником руководящих указаний по разработке системных профилей защиты и заданий по безопасности.

В число других использованных документов также вошли NIST SP 800-53A «Руководство для проверки эффективности средств управления безопасностью в федеральных информационных системах» и немецкое «Руководство по базовой защите ИТ».

Рисунок 3 – Соотношение между средой эксплуатации и критериями оценки

Необходимые концепции и конкретные средства управления были адаптированы из данных документов. Однако авторы отмечают, что критерии оценки не предназначены для определения того, каким образом можно обеспечить безопасность проектирования и управления эксплуатирующимися системами. Они определяют, как оценить безопасность эксплуатирующихся (автоматизированных) систем с использованием тех свидетельств, которые могут предоставить оценщикам владельцы, разработчики, интеграторы, операторы и администраторы систем. Поэтому аспекты, охватываемые критериями оценки, и их акцент отличаются от исходных материалов, содержащихся в стандартах и руководствах, использованных в качестве источников разработки.

В отчете также отмечается, что в связи с базированием процессов, документов и задач, определенных в проекте ISO/IEC TR 19791, на существующих эквивалентах из стандарта ISO/IEC 15408, материалы отчета, заимствованные из других стандартов и руководств, были преобразованы к формату, который представляет собой расширение формата уже используемого в стандарте ISO/IEC 15408.

Приведем некоторые пояснения о взаимоотношении материалов проекта ISO/IEC TR 19791 и материалов других используемых в нем стандартов по ИБ, представленных в тексте проекта отчета.

Международный стандарт ISO/IEC 17799 является кодексом установившейся практики, содержащим рекомендованные средства управления безопасностью для организаций, позволяющие осуществлять менеджмент безопасности информационных активов. Этот стандарт дает рекомендации по менеджменту ИБ в части инициирования, реализации и поддержки ИБ в организации (очевидно, что упоминая ISO/IEC 17799, авторы рассматриваемого

технического отчета имеют в виду также и вторую часть британского стандарта BS 7799-2).

Также стандарт ISO/IEC 17799 предоставляет широко принятую структуру менеджмента для управления операционной безопасностью. При разработке проекта отчета ISO/IEC TR 19791 его авторы использовали данный стандарт в качестве основного источника для идентификации и спецификации тех аспектов операционной безопасности, где требовались соответствующие средства управления (защитные меры).

Специальная публикация NIST SP 800-53 содержит руководящие указания по выбору и определению средств управления безопасностью для информационных систем (систем ИТ) и предназначена для применения в правительственных федеральных информационных системах США. Некоторые части данной специальной публикации при определении средств управления безопасностью опираются на материалы стандарта ISO/IEC 17799, но она также охватывает и другие области, которые не связаны напрямую с менеджментом ИБ. На основании этого публикация NIST SP 800-53 была использована в качестве второго основного источника для формирования операционных средств управления, особенно в тех областях обеспечения операционной безопасности, которые не охвачены международным стандартом ISO/IEC 17799.

Несмотря на имеющиеся вопросы в части целей и задач практического применения технического отчета ISO/IEC TR 19791 принятие его в ИСО запланировано на начало 2006 года. Также в перспективных планах работ WG3 SC27 от апреля 2005 года отмечается возможность изменения в ближайшем будущем типа разрабатываемого документа с «технического отчета» на «международный стандарт» [23]. Данная возможность, как отмечается, обусловлена важностью и сложностью затронутой предметной области, а также проработкой этого направления до такого уровня, который приближается к уровню международного стандарта.

Подводя некий итог обзору и анализу проекта документа ИСО ISO/IEC TR 19791 «Оценка безопасности эксплуатирующихся систем» можно сделать следующие выводы:

– документ, безусловно, представляет определенную практическую ценность для собственников как некий вариант видения направления сближения технического направления стандартизации (ISO/IEC 15408) и стандартизации на уровне менеджмента ИБ в организации ISO/IEC 17799;

– несмотря на высокую активность и продуктивность проведения работ проект ISO/IEC TR 19791 является все еще недостаточно проработанным для эффективного практического применения. Это, в первую очередь, связано с неясностью целей оценки и сертификации эксплуатирующихся систем, отсутствием проработки процедур взаимодействия спонсора оценки, оценщиков и органов сертификации и отсутствием методологии оценки безопасности эксплуатирующихся систем по требованиям данного технического отчета.

Указанные выводы в значительной мере перекликаются с результатами анализа ISO/IEC TR 19791, приведенными в [20], где наряду с отмеченными вопросами приведены и более детальные проблемы, решение которых в будущем предопределит практический успех документа (например, сроки проведения оценки, сроки и условия сохранения действия результатов оценки и т.д.).

Российская действительность

Как уже отмечалось, в апреле 2002 года был принят российский аналог ISO/IEC 15408:1999 – ГОСТ Р ИСО/МЭК 15408-2002 с датой введения его в

действие через полтора года – с 1 января 2004 года. Полуторалетний период с момента принятия стандарта до ввода в действие был отпущен на формирование основы его применения в России. Основой применения стандарта должно было быть принятие по линии гармонизации соответствующей методологии оценки безопасности ИТ и нормативных (руководящих) документов для новой системы оценки согласно принятой на уровне ИСО модели и контекста оценок (см. рисунок 2). Что же было достигнуто к 2004 году.

На 1 января 2004 года в силу ряда причин так и не была развернута полноценно действующая система оценки и сертификации по требованиям введенного стандарта ГОСТ Р ИСО/МЭК 15408. Не была введена официально в действие методология оценок по требованиям ГОСТ Р ИСО/МЭК 15408, хотя отдельные оценки и производились и выдавались некие итоговые документы, имеющие наименование «Сертификат», но неясного статуса. Не был принят практически ни один документ, дающий спонсору оценок (заинтересованной стороне, осуществляющей финансирование всех работ) или потребителю сертифицированного по безопасности продукта ИТ, например, собственнику системы ИТ или АС, каких-либо внятных руководств по использованию ГОСТ Р ИСО/МЭК 15408 и оцененных по нему продуктов ИТ в его интересах. В то же время был подготовлен и продолжает расширяться состав документов для ГОСТ Р ИСО/МЭК 15408, направленных на разработчика продукта ИТ или органы оценки и сертификации.

На начало 2006 года ситуация, к сожалению, не претерпела кардинальных отличий от двухлетней давности. К настоящему времени подготовлен и частично утвержден следующий перечень нормативно-методических документов, предназначенных для поддержки оценок безопасности продуктов и систем ИТ по требованиям Руководящих документов на основе ГОСТ Р ИСО/МЭК 15408-2002 (см. таблицу 1, источник – официальный Интернет-сайт ФСТЭК, *http://www.fstec.ru/*).

Таблица 1 – Документы ФСТЭК в поддержку оценок безопасности ИТ на основе ГОСТ Р ИСО/МЭК 15408-2002

Наименование	Год утверждения	Основа разработки (международные документы)
Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности	2003	Нет сведений
Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты	2003	Фактически перевод стандарта ISO/IEC 15292-2001, Information technology – Security techniques – Protection Profile registration procedures, но для Российского применения
Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты	2003	Нет сведений
Руководство по разработке профилей защиты и заданий по безопасности	2003	На основе одной из ранней (2002 года) версии проекта, технического отчета ISO/IEC TR 15446-2004, которая в последующем претерпела существенные изменения
Проект руководящего документа «Общая методология оценки безопасности информационных технологий»	планируется к утверждению	«Общая методология оценки безопасности ИТ», версия 1.1a, апрель 2002 г.
Проект типовой методики оценки профилей защиты и заданий по	планируется к	«Общая методология оценки безопасности ИТ. Часть 2:

Наименование	Год утверждения	Основа разработки (международные документы)
безопасности	утверждению	Методология оценки», версия 1.0, CEM-99/045, август 1999 г.

В начале 2006 года на рассмотрение заинтересованных сторон были также направлены очередные редакции проектов от 2005 года следующих Руководящих документов ФСТЭК России:

– «Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности»;

– «Руководящий документ. Безопасность информационных технологий. Руководство по разработке профилей защиты и заданий по безопасности»;

– «Руководящий документ. Безопасность информационных технологий. Положение по обеспечению безопасности в жизненном цикле изделий информационных технологий»;

– «Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты»;

– «Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты»;

– «Руководящий документ. Безопасность информационных технологий. Типовые модели угроз безопасности информационных технологий автоматизированных систем критического применения»;

– «Базовая модель угроз безопасности информационных технологий».

Таблица 1 и приведенный перечень показывают следующее.

Во-первых, часть РД в поддержку оценок безопасности ИТ не имеют прямых аналогов ни среди документов ISO/IEC, ни среди документов национальных систем оценки соответствия по ОК других стран, которые осуществляют такие оценки с 1998 года (*http://www.commoncriteriaportal.org/*). Может быть, это и могло бы быть оправдано практическими потребностями для собственников и владельцев систем ИТ, однако полезных для них практических руководств документы не содержат, так как преимущественно ориентированы на разработчиков и/или оценщиков продуктов ИТ и органы сертификации.

Во-вторых, проект РД «Общая методология оценки безопасности информационных технологий» и проект типовой методики оценки профилей защиты и заданий по безопасности основаны на крайне устаревших и выведенных из использования версиях аналогичных документов CCDB (международного органа по развитию ОК). Распространенная в начале 2006 года версия проекта РД «Общая методология оценки безопасности информационных технологий» хотя и расширена (231 страница против 184) относительно версии документа, размещенной на *http://www.fstec.ru/_licen/014.pdf*, однако также основывается на выводимых из действия зарубежных аналогах. Международная система оценки по ОК, например, на данный момент работает по версии 2.2 (заменившей версию 2.1) Общей методологии оценки от января 2004 года или по международному стандарту ISO/IEC 18045-2005, а проекты РД согласно информации в «Предисловии» к документам основываются на версии 1.1а Общей методологии оценки от 2002 года.

В-третьих, что касается РД «Руководство по разработке профилей защиты и заданий по безопасности», то в отсутствии в документе точных ссылочных данных, анализируя текст документа можно предположить, что он также основан на переводе устаревшей, и имеющей массу дефектов, версии проекта технического отчета ISO/IEC TR 15446 «Информационные технологии. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты

и заданий по безопасности» от 2002 года. Данная версия в последующем подверглась существенному пересмотру. При этом, еще в 2004 году ISO/IEC была принята и введена в действие окончательная версия данного технического отчета и он в настоящее время уже находится в стадии очередного пересмотра в контексте очередного ведущегося пересмотра уже второй редакции ISO/IEC 15408 от 2005 года.

Таким образом, нормативно-методическая база для поддержки оценок безопасности ИТ по требованиям ГОСТ Р ИСО/МЭК 15408-2002, введенная в действие в 2003 году, на настоящий момент значительно устарела и не отражает фактического состояния дел мирового сообщества в данной области, что непременно приведет к проблемам для собственников систем ИТ в контексте грядущего вступления России во Всемирную торговую организацию (ВТО). Это же в равной мере относится и к планируемым для утверждения проектам документов, которые, еще будучи не принятыми, уже фактически устарели. Нет никаких сведений о поддержке и внедрении ФСТЭК новых, соответствующих международным нормам, нормативно-методологических документов в России. По всей видимости, это порождено отсутствием процессов по быстрому реагированию в России на пересмотр документов международного уровня. В заключение данного раздела статьи, к сожалению, можно констатировать, что заявления о том, что Россия работает по международным стандартам при ближайшем рассмотрении показывает их несостоятельность.

Интеграция России в мировую экономику и безопасность ИТ

Отмеченные соображения, относительно того, что существующая в России ситуация приведет к проблемам для собственников систем ИТ в контексте грядущего вступления России в ВТО, не безосновательны. И обусловлено это следующим.

В декабре 2002 года был принят ФЗ № 184 «О техническом регулировании» (далее по тексту 184-й Закон), целью принятия которого являлось сближение национального законодательства с международным через определение того, какие требования в технической сфере могут носить обязательный характер, а какие нет. Принятие 184-го Закона стало результатом переговоров о вступлении России в ВТО, в частности реализации в России положений Соглашения ВТО о технических барьерах в торговле (ТБТ). 184-ый Закон регулирует (согласно статьи 1) отношения, возникающие при:

– разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;

– разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;

– оценке соответствия.

При этом 184-ый Закон также определяет права и обязанности участников регулируемых Федеральным законом отношений.

С принятием данного Федерального закона кардинально изменилось национальное правовое поле в технической сфере, в том числе и в области безопасности ИТ. Основной формой выражения обязательных требований согласно 184-ого Закона определены общие и специальные технические регламенты, имеющие статус Федеральных законов. Все национальные стандарты согласно 184-му Закону получили статус добровольных, отраслевые стандарты

были отменены, а их ниша была заменена стандартами организаций, где под организациями определены, в том числе, и коммерческие, общественные, научные организации, саморегулируемые организации, объединения юридических лиц.

Однако область информационной безопасности не вошла в перечень вопросов (направлений) безопасности, регулируемых 184-ым Законом, по которым могут приниматься общие и развивающие их специальные технические регламенты. То есть отсутствует правовая база для разработки общего и развивающего его специального технического регламента (одного или нескольких), которые бы определили бы базу обязательных требований в части безопасности ИТ.

Это привнесло свою, что называется, «определенную неопределенность», т.к. с одной стороны п. 2.2 Соглашения о ТБТ предполагает возможность законодательного регулирования странами всех необходимых вопросов, касающихся национальной безопасности, а область информационной безопасности является именно таковой согласно «Концепции национальной безопасности Российской Федерации». В то же время регулирование вопросов защиты информации и информационной безопасности затронуто лишь в статье 5 184-ого Закона. Данная статья 184-го Закона определяет порядок технического регулирования в отношении оборонной продукции (работ, услуг) и продукции (работ, услуг), сведения о которой составляют государственную тайну.

Тем не менее, в федеральную программу разработки технических регламентов на период 2004–2006 гг. была включена разработка проектов таких специальных технических регламентов (СТР), как «Безопасность информационных технологий», «О требованиях к средствам обеспечения безопасности информационных технологий», которые и были разработаны в период с апреля по сентябрь 2005 года в соответствии с государственными контрактами на разработку технических регламентов РТР-08-45 и РТР-08-46. Разработчиком по госконтрактам формально выступил НИИ «Восход», а фактически, как показали общественные слушания документов – головные организации-разработчики направления Общие критерии от ФТСЭК России.

Как нетрудно предположить, что основой указанных СТР явились рассмотренные выше Руководящие документы ФСТЭК России из направления Общие критерии, а также положения подробно рассмотренного ранее технического отчета ИСО – ISO/IEC 19791 со всеми его достоинствами и недостатками. Здесь следует отметить, что нигде в мире международный стандарт ISO/IEC 15408, исходя из его узкой, технической направленности, не введен на уровне законодательства. Существующие зарубежные законодательные требования, например, в США и странах Западной Европы, определяют лишь необходимость сертификации продуктов ИТ и не во всех возможных случаях, а преимущественно при взаимодействии систем ИТ организаций с государственными системами, но не затрагивают вопросы того, как и что должно представляться и оцениваться при сертификации.

Несмотря на это разработчики проектов СТР «Безопасность информационных технологий», «О требованиях к средствам обеспечения безопасности информационных технологий» практически полностью воспроизвели структуру требований ISO/IEC 15408 в его первой редакции от 1999 года и других отдельных документов в тексте проектов СТР. Указанное не может не вызывать беспокойства собственников и пользователей систем ИТ, так как с одной стороны разработчиками проектов СТР было публично признано на общественных слушаниях документов, что в данном виде регламенты распространяются фактически на любую компьютерную систему в РФ, с другой

же стороны, и это известно специалистам, ветка международных стандартов ИСО по оценке безопасности ИТ неуклонно развивается, и первая редакция международного стандарта ISO/IEC 15408, которая использовалась при подготовке российского ГОСТ Р ИСО/МЭК 15408-2002 и проектов СТР, уже в 2005 году была выведена из действия на международном уровне в связи с принятием второй редакции документа. При этом в 2006 году планируется принять третью редакцию международного стандарта, оценки безопасности ИТ, по которой будут несовместимы с оценками по первой и второй редакциям документа. Таблица 2 иллюстрирует основные изменения в структуре функциональных требований трех редакций международного стандарта ISO/IEC 15408.

Таблица 2 - Состав классов функциональных требований безопасности в редакциях международного стандарта ISO/IEC 15408.

Классы функциональных требований в редакциях 1 (1999) и 2 (2005) ISO/IEC 15408	**Классы функциональных требований в редакции 3 (2006) ISO/IEC 15408**
FAU. Аудит безопасности	FAU. Аудит
FCO. Связь	FCO. Связь
FCS. Криптографическая поддержка	—
FDP. Защита данных пользователя	FDP. Защита данных и приватность
FIA. Идентификация и аутентификация	FIA. Идентификация, аутентификация и связывание
FMT. Управление безопасностью	—
FPR. Приватность	—
FPT. Защита функций безопасности объекта оценки	FPT. Защита функций безопасности объекта оценки
FRU. Использование ресурсов	—
FTA. Доступ к объекту оценки	—
FTP. Доверенный маршрут/канал	—
—	FMI. Дополнительное

В настоящее время работы по продвижению проектов специальных технических регламентов «Безопасность информационных технологий», «О требованиях к средствам обеспечения безопасности информационных технологий» временно приостановлены, однако пути нахождения консенсуса в вопросах оценок безопасности ИТ в том виде, как они могли бы быть полезны потребителям, не просматриваются и пока что не ясны.

Затрагивая вопросы совершенствования национального законодательства нельзя не отметить, что 184-ый Закон потенциально затрагивает и регулирует только часть вопросов, которые касаются области ИТ. Другая же часть задач области ИТ – область телекоммуникаций и связи в силу исторически сложившейся национальной практики рассматривалась обособлено, и разработчики 184-ого Закона не смогли изменить эту ситуацию. Пункт 2 Статьи 1 184-ого Закона определяет, что:

> *«Требования к функционированию единой сети связи Российской Федерации и к продукции, связанные с обеспечением целостности, устойчивости функционирования указанной сети связи и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи Российской Федерации и использованием радиочастотного спектра, соответственно устанавливаются и регулируются законодательством Российской Федерации в области связи»*

На деле это нашло отражении в принятии в 2003 году Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» (далее 126-й Закон). Для практического применения 126-ого Закона был определен состав подзаконных актов (свыше 20),

которые обеспечивают реализацию положений документа, в том числе и в части оценки соответствия средств и систем связи, обеспечения безопасности и устойчивости функционирования средств и систем связи. В настоящее время, например, приняты следующие Постановления Правительства РФ, так или иначе затрагивающие вопросы безопасности средств и систем связи:

№ 328 от 25 мая 2005 г. «Об утверждении Правил оказания услуг подвижной связи»;

№ 310 от 18 мая 2005 г. «Об утверждении Правил оказания услуг местной, внутризоновой, междугородной и международной телефонной связи»;

№ 214 от 13 апреля 2005г. «Об утверждении Правил организации и проведения работ по обязательному подтверждению соответствия средств связи»;

№ 165 от 29 марта 2005 г. «Об утверждении Правил аккредитации органов по сертификации, испытательных лабораторий (центров), проводящих сертификационные испытания средств связи»;

№ 110 от 2 марта 2005 г. «Об утверждении Порядка осуществления государственного надзора за деятельностью в области связи»;

№ 896 от 31 декабря 2004 г. «Об утверждении перечня средств связи, подлежащих обязательной сертификации»;

№ 318 от 30 июня 2004 г. «Об утверждении Положения о Федеральной службе по надзору в сфере связи» и другие.

В то же время на уровне ИСО в силу очевидных практических потребностей область ИТ уже достаточно давно рассматривается неразрывно с областью телекоммуникаций, что получило общее наименование «информационно-телекоммуникационные технологии». Практические работы по стандартизации в этой области проводятся в теснейшем взаимодействии ИСО с Международным союзом электросвязи (МСЭ) с его секретариатом в области телекоммуникаций. Примерами тому можно привести международный стандарт ISO/IEC 13335 «*Information Technology. Security techniques. Management of information and communications technology security*», стандарты по реализации механизмов безопасности, разработанные совместно ИСО и МСЭ и также имеющие двойную нумерацию: ISO/IEC 14516/X.842, ISO/IEC 15816/X.841, ISO/IEC 15945/X.843, ISO/IEC 18028-2/X.805 и другие документы.

В этой связи продолжающееся в России искусственное разделение на области «связь»-«не связь» порождает ситуацию, красноречиво иллюстрируемую русской пословицей «у семи нянек дитя без глазу». В настоящее время в стране на государственном уровне к задачам защиты информации, информационной безопасности и безопасности ИТ (все три из перечисленных сущностей имеют много общего, как по целям, так и способам их достижения) имеют в той или иной мере отношение: ФСБ России (преимущественно криптография), ФСТЭК России (защита информации), Министерство по информационным технологиям и связи (безопасность ИТ), Совет безопасности России (информационная безопасность) и другие структуры. Практически все из перечисленных госструктур издают свои нормативные акты и Федеральные законы, затрагивающие задачи защиты информации, информационной безопасности и безопасности ИТ, участвуют в разработке национальных стандартов, как на основе международных, так и не имеющих аналогов за рубежом. При этом каждое из ведомств идет своим путем и мало заботиться о целостности и непротиворечивости формируемой нормативной и правовой базы.

Например, в проект национального стандарта ГОСТ Р «Защита информации. Обеспечение безопасности информации сетей электросвязи. Общие положения», разработанного в 2005 году, было включено понятие «угроза безопасности сети электросвязи», которое определялось как:

«возможное воздействие нарушителя на инфокоммуникационную структуру сети электросвязи, создающее потенциальную или реально существующую опасность нанесения ущерба интересам пользователей услугами связи, операторов связи и/или органов государственной власти»,

что ограничивает возможный спектр источников угроз только лишь до действий людей. Это противоречит реальному состоянию дел и положениям международных стандартов, где, например, в ISO/IEC 13335-1-2004 *«Information Technology. Security techniques. Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management»* определено, что «угроза» есть:

«потенциальная причина инцидента, который может нанести ущерб системе или организации».

Примеров подобных расхождений как национальной нормативной базы с международной, так и документов национальной нормативной базы между собой масса и их можно продолжить.

Спасение утопающих – дело рук самих утопающих

При всей имеющейся сложности «текущего момента» собственникам и пользователям систем ИТ, автоматизированных систем требуются практические решения и не в будущем, а сейчас, обеспечивающие их потребности в решении задачи обеспечения информационной безопасности. При этом практика эксплуатации и статистика показывают, что задачи обеспечения информационной безопасности зачастую решаются и гораздо более эффективно (по соотношению стоимость/результат) нетехническими методами: организационными, административными, технологическими. Из практики крупных организаций известно, что, будучи установленным в действующую систему ИТ или АС любое техническое средство безопасности даже будучи сертифицированным по высочайшему классу через непродолжительный период времени, как правило 1-3 месяца, становиться «прозрачным» практически для всех пользователей АС. И это не дефект средства безопасности – а специфика его эксплуатации. Средство безопасности по своему назначению налагает ограничения – ставит барьеры – на деятельность персонала организации и внешних пользователей, которые всеми правдами и неправдами пытаются их преодолеть или же нейтрализовать для обеспечения свободы в действиях.

Поэтому сертификация изделий ИТ с практической точки зрения, будь то отдельный продукт ИТ, например, межсетевой экран или средство управления доступом, или система ИТ для собственников этих систем может служить только лишь источником сведений о потенциальных возможностях сертифицированного изделия ИТ и не более. На практике же все определяется реальной средой безопасности в организации, на которую влияют и определяют ее состояние корпоративные политики информационной безопасности, действующие формализованные правила и положения в части обеспечения информационной безопасности, организация контроля за соблюдением требований внутренних нормативных актов в каждой конкретной организации. Другими словами все определяется системой управления (менеджмента) информационной безопасности организации и тем, насколько данная система менеджмента информационной безопасности отвечает потребностям бизнеса организации и ожиданиям топ-менеджмента организации. Указанные вопросы в подавляющем большинстве лежат в плоскости организационно-административной деятельности, и ни один из действующих в России нормативных актов в области защиты информации,

информационной безопасности и безопасности ИТ и действующих стандартов не рассматривают данных вопросов. При этом все большее число российских компаний соприкасается с международной деятельностью и требованиями партнеров по бизнесу в части обеспечения информационной безопасности в соответствии с действующими международными нормами и правилами.

Реальным выходом из сложившейся ситуации для организаций может быть принятие своих собственных стандартов обеспечения информационной безопасности, тем более что такая форма выражения требований предусмотрена 184-м Законом в виде «стандартов организации».

По этому пути пошли ряд организаций из различных отраслей деятельности. Например, Банк России с 2002 года разрабатывает банковский стандарт обеспечения информационной безопасности организаций банковской системы Российской Федерации (БС РФ). Вторая редакция стандарта была введена в действие в январе 2006 года – СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (см. «Вестник Банка России» №6 (876) от 3.02.2006). Стандарт не заменяет действующие требования по технической защите информации, а ориентирован на:

– повышение доверия к банковской системе РФ;

– повышение стабильности функционирования организаций БС РФ и на этой основе – стабильности функционирования БС РФ в целом;

– достижение адекватности мер по обеспечению ИБ реальным угрозам;

– предотвращение и/или снижение ущерба от инцидентов ИБ;

– установление единых требований по обеспечению ИБ организаций БС РФ;

– повышение эффективности мероприятий по обеспечению и поддержанию ИБ организаций БС РФ;

– предоставление результатов оценки уровня ИБ различных организаций в сопоставимом виде.

В стандарте определены основные требования по управлению информационной безопасностью на уровне организации, а также и другие более специфичные вопросы, включая общие требования по обеспечению информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла. Стандарт разработан на основе национальных и международных стандартов, таких как:

– ГОСТ Р 1.4-2004 Стандартизация в Российской Федерации. Стандарты организаций. Общие положения;

– ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;

– ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты;

– ГОСТ Р ИСО 9001-2001 Система менеджмента качества. Требования;

– ГОСТ Р ИСО/МЭК 15408-1÷3-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий;

– ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств;

– ГОСТ Р ИСО/МЭК ТО 15271-2002 Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств);

– ISO/IEC IS 13335-1÷2 *Information Technology. Security techniques. Management of information and communications technology security*;

– ISO TR 13569 *Banking and related financial services. Information security guidelines*;

– ISO/IEC IS 15288-2002 *Systems engineering. System Life Cycle Processes*;

– ISO/IEC TR 15504-1÷5 *Information technology. Process assessment*;

– ISO/IEC TR 18028-1÷5 *Information technology. Security techniques. IT network security*;

– ISO/IEC TR 18043 *Information technology. Selection, deployment and operations of intrusion detection systems* (*IDS*);

– ISO/IEC TR 18044-2004 *Information Technology. Security techniques. Information security incident management*;

– ISO/IEC IS 17799-2005 (*second edition*) (с 2007 года – ISO/IEC IS 27002) *Information Technology. Code of practice for information security management*;

– ISO/IEC IS 27001-2005 *Information technology. Security techniques. Information security management systems. Requirements*.

В силу рассмотренных выше причин в настоящее время затруднительно прогнозировать направления развития национальной нормативной базы в области защиты информации, информационной безопасности и безопасности ИТ, а следовательно и то, какой из существующих зарубежных стандартов, ориентированных на обеспечение или оценку безопасности систем ИТ или же автоматизированных систем, может быть полезен конкретному собственнику и в какой мере. В отсутствии консенсуса на уровне государства по данной проблематике в конечном итоге «крайними» всегда останутся собственники систем, и выбирать им из имеющегося особенно нечего. По всей видимости, на ближайшую перспективу собственниками систем ИТ и АС придется решать проблемы обеспечения информационной безопасности самим самостоятельно или же во взаимодействии с партнерами по бизнесу/отрасли через принятие в сообществах согласованных и единых норм и правил, в формах подобной стандарту организации, которые должны будут учитывать действующие на текущий период национальные требования и расширять их теми требованиями, которые диктуются бизнесом и бизнес-сообществом.

ЛИТЕРАТУРА:

1. ISO/IEC 15408:1999(E) *Information technology – Security techniques – Evaluation criteria for IT security, First edition*, *First edition*, 1999-12-01.
2. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. – М.: Воениздат, 1992.
3 Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – М.: Воениздат, 1992.
4. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. – М.: Воениздат, 1992.
5. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации.

Классификация автоматизированных систем и требования по защите информации. – М.: Воениздат, 1992.
6. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. – М.: Воениздат, 1992.
7. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – М., 1997.
8. Трубачев А.П., Долинин М.Ю. и др. Оценка безопасности информационных технологий. Серия «Безопасность информационных технологий». – М.: СИП РИА, 2001. – 356 с.
9. Сидак А.А. Формирование требований безопасности современных сетевых информационных технологий. Серия «Безопасность информационных технологий». – М.: МГУЛ, 2001. – 278 с.
10. Общие критерии оценки безопасности информационных технологий: Учебное пособие. Перевод с английского Е.А. Сидак/Под ред. М.Т. Кобзаря, А.А. Сидака. – М.: ЦБИ, 2001. – 81 с.
11. «Интервью заместителя начальника отдела лицензирования и сертификации Гостехкомиссии России Калайды И.А.» // «Jet Info», №8 (87/2000).
12. ISO/IEC 17799:2000 *Information technology – Code of practice for information security management*.
13. BS 7799-2:2002 *Information security management systems – Specification with guidance for use*.
14. Голованов В.Б., Каминский В.Г., Алексеев В.М. «Стандарты ИСО/МЭК 15408 и ИСО/МЭК 17799: что дальше? К вопросу об оценке безопасности эксплуатирующихся систем» // «Защита информации. Конфидент», №4 (58) 2004, с. 70-73.
15. ISO/IEC JTC 1/SC 27/WG 3 №607, *Use of BS 7799-2 and ISO/IEC 17799 in Operational System Evaluation*, 9.03.2003.
16. ISO/IEC JTC 1/SC 27 №3169 «*Officer's contribution for study period on Systems Evaluation*», 8.04.2002.
17. ISO/IEC JTC 1/SC 27 N 3396 «*System Evaluation, Principles, Concepts, Terms*», 09.10.2002.
18. ISO/IEC JTC 1/SC 27/WG 3 N 610 «*Security Assessment of Operational Systems*», 09.04.2003.
19. ISO/IEC JTC 1/SC27 N 4246. ISO/IEC 2nd PDTR 19791 «*Information technology – Security techniques – Security assessment of operational systems*».
20. «Оценка безопасности автоматизированных систем» Обзор и анализ предлагаемого проекта технического доклада ISO/IEC PDTR 19791 // «Jet Info», №7 (146/2005).
21. ISO/IEC JTC 1/SC 27/WG 3 N 781 «*Dispositions of comments on ISO/IEC Second PDTR* 19791 (SC 27 N 4246): *Information technology – Security techniques – Security assessment of operational systems* ». 2005-04-12.
22. ISO/IEC JTC 1/SC 27/WG 3 N 790 «*Meeting Report – Meeting No. 30 11th to 15th April, 2005 Vienna, Austria*». 2005-05-06.
23. ISO/IEC JTC 1/SC 27/WG 3 N 771rev1 «WG 3 Road Map». 15.04.2005.

Получено 27.12.2005. Опубликовано в Internet 29.12.2005.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 6. С.101-102. Секция-4: Анализ вычислительной среды, верификация, сертификация программ.
Пенза-2005 (http://beda.stup.ac.ru/RV-conf/v06/022)

ОПРЕДЕЛЕНИЕ ДЛИТЕЛЬНОСТИ ПЕРЕХОДНЫХ ПРОЦЕССОВ В ДИСКРЕТНОЙ СИСТЕМЕ СИНХРОНИЗАЦИИ (N+1)-ГО ПОРЯДКА

Лысиков А.В.
ФГУП "ПНИЭИ"

Как показано в работе [1], эффект разделения на N тактов моментов определения и использования синхроинформации в математической модели эквивалентен включению последовательно с цифровым фильтром системы звена задержки на N тактов дискретизации.

При отсутствии шума ($n_{ш} = 0$) разностное уравнение ДСС первого порядка с задержкой можно записать в виде[1]:

$$\psi[k] - \psi[k-1] + \alpha \sin(\psi[k-N-1]) = \varphi[k] - \varphi[k-1], \qquad (1)$$

где $\psi[k] = \varphi[k] - \hat{\varphi}[k]$; $\varphi[k]$ и $\hat{\varphi}[k]$ − фазы соответственно входного и подстраиваемого колебаний; $n_{ш}[k]$ – отсчеты дискретного шума на выходе фазового дискриминатора ДСС; α − коэффициент, определяющий свойства ДСС.

Трудность анализа подобных систем обусловлена высоким порядком описывающих их разностных уравнений. Определённые выводы о характере поведения ДСС с задержкой могут быть сделаны на основе рассмотрения линеаризованной модели [2]. Получение более полной информации об их свойствах возможно с помощью численного моделирования. Данный подход и использован в настоящей работе.

В работе [2], было показано, что стационарное значение фазовой ошибки $\psi_{N1стn}$ не зависит от порядка задержки N и равно:

$$\psi_{N1стn} = \arcsin(\omega_{0r}/\alpha) + 2\,\pi\,n, \qquad n \text{ – любое целое.} \qquad (2)$$

Рассмотрим часто встречающуюся на практике ситуация, когда частота входного сигнала сдвинута относительно своего номинального значения на величину f_r. При

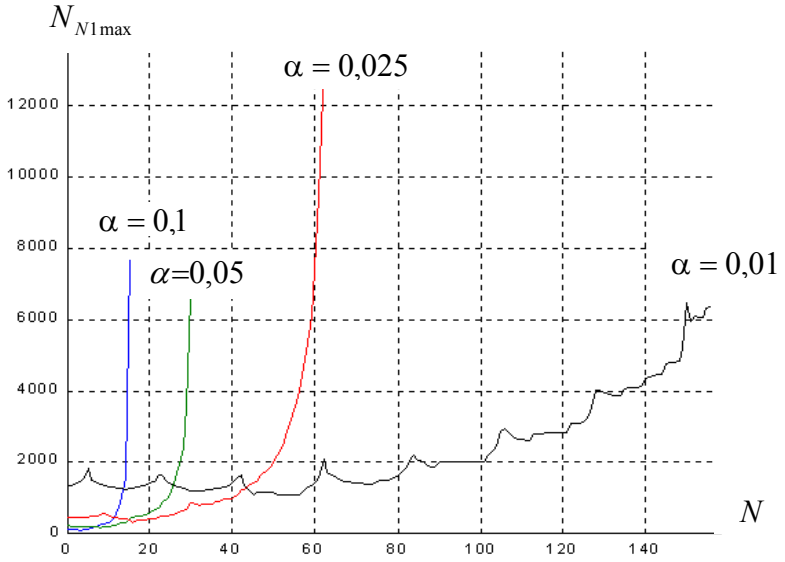

Рис. 1

этом фаза задающего колебания $\varphi[k]$ изменяется по линейному закону: $\varphi[k] = \omega_{0r}\,k$, $\omega_{0r} = 2\,\pi\,f_r/f_д$.

Исследование зависимости длительности переходного процесса, выраженной в числе тактов дискретизации $N_{\text{ппN1}}$, от порядка задержки N, проводилось на основе численного решения нелинейного разностного уравнения (1). При этом величина $N_{\text{ппN1}}$ оценивалась по интервалу между запуском системы и моментом, когда фазовая ошибка $\psi[k]$ отличалась от определяемого соотношением (2) стационарного значения не более, чем на 0,1 градуса (или на $\pi/1800$ радиан). Относительная начальная частотная расстройка f_{0rN1} задавалась равной 0,001 (что соответствует, например, $f_r = 9{,}6$ Гц при $f_{\text{д}} = 9600$ Гц). При каждом значении N оценка $N_{\text{ппN1}}$ производилась при различных начальных фазовых сдвигах $\psi[0]$, последовательно выбираемых из диапазона $0 \div 2\pi$ с шагом $\pi/30$. В качестве характеристики длительности переходного процесса принималось максимальное значение $N_{N1\max} = \max\limits_{\psi[0]} N_{\text{ппN1}}$. Полученные таким образом зависимости $N_{N1\max} = F_{\text{ппN1}}(N)$ представлены на рис. 1.

Из графиков видно, что при малых N изменение длительности переходного процесса, обусловленное наличием задержки, является незначительным, однако с ростом N имеется устойчивая тенденция к существенному её увеличению.

Немонотонность отдельных участков кривых вызвана сложным характером соответствующего изменению N перераспределения значений модулей корней характеристического уравнения, которые и определяют динамические свойства системы. Вместе с тем по мере приближения к границе устойчивости, имеющей место при N равном $N_{1\max}$,задаваемому соотношением [3]

$$N_{1\max} = \left[0{,}5\,\pi / \left[2\arcsin(\alpha/2)\right] - 1\right]_{\text{ц. ч.}}, \qquad (3)$$

модули доминирующих корней [3][6] принимают значения, близкие к 1. Следствием этого и является иллюстрируемое графиками рис. 1 резкое увеличение максимальной длительности переходного процесса.

Неодинаковая протяженность изображенных на рис. 1 графиков вдоль оси абсцисс обусловлена задаваемой (3) зависимостью $N_{1\max}$ от α.

ЛИТЕРАТУРА:

1. *Лысиков А.В.* Математические модели дискретных систем синхронизации с разделенными моментами выделения и использования синхроинформации. / *А.В.Лысиков, В.А.Фунтиков, М.С.Кирюхин, Б.В.Султанов* – Научно-технический сборник «Специальная техника средств связи». выпуск 2. Пенза 2005. ФГУП «ПНИЭИ» …….

2. *Лысиков А.В.* Исследование дискретных систем синхронизации (N+1)-го порядка с разделением на N тактов моментов определения и использования синхроинформации при отсутствии шума. / *А.В.Лысиков*– Научно-технический сборник «Специальная техника средств связи». выпуск 2. Пенза 2005. ФГУП «ПНИЭИ» …….

3. *Попов Е. П.* Теория линейных систем автоматического регулирования и управления. – М.: Наука, 1989. – 304 с.

[6] Следуя терминологии, принятой в работе [3], доминирующими будем называть корни характеристического уравнения с наибольшими модулями. У асимптотически устойчивых систем они являются ближайшими к единичной окружности и расположены внутри неё.

СОДЕРЖАНИЕ

Труды научно-технической конференция
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Том 6
Пенза – 2005 г.

ЛР № 020779

Подписано к печати 28.04.2005 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