ОСОБЕННОСТИ ТЕХНОЛОГИИ БИОМЕТРИЧЕСКОЙ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

УДК: 004.032.26, 004.424.47

Майоров А.В

Рассмотрены существующие схемы защиты исполняемого кода. Предложено использовать нечеткие биометрические данные, дополнив программное обеспечение высоконадежными преобразователями биометрия-код. Описаны 3 способа биометрической защиты: с размножением ключа, с трансляцией исполняемых кодов и с контролем вероятностей ошибок первого и второго рода.

Большинство систем защиты программного обеспечения использует ключи. При этом уязвимыми местами таких систем являются процедуры хранения ключей, а также процедуры сравнения ключей с эталонными. Известно множество примеров, когда злоумышленникам достаточно разработать заплатку на программные модули и свободный доступ всем желающим к программе будет обеспечен. Принципиальная схема программно-криптографической защиты, включающей в себя как ограничение доступа к исполняемому коду по ключу, его шифрование (маскировку), а также блочно-семантическое связывание, показана на Рис. 1.

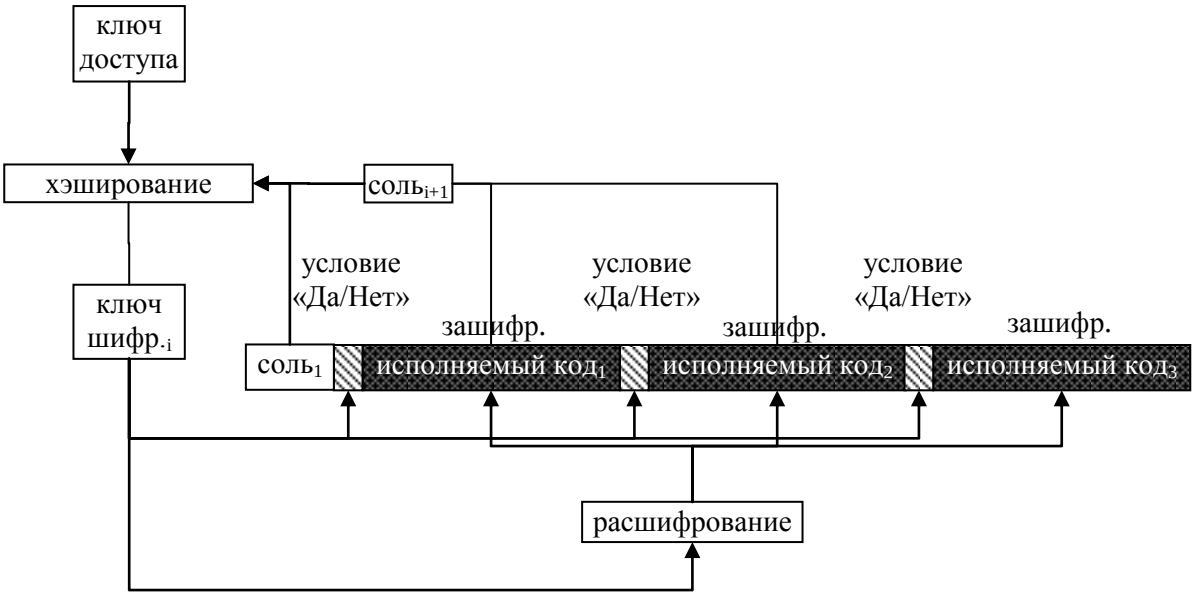

Рис 1. Схема блочного шифрования исполняемого кода с контролем доступа

Основными уязвимыми местами предложенной схемы в массовых системах являются:

1. *ключ доступа*, для которого можно организовать атаку перехвата;
2. *однобитовое условие «Да/Нет»*, которое можно изменить инверсией бита, операции сравнения и другими подобными методами;
3. *исполняемый код*, который становится известным, после покупки злоумышленниками хотя бы одной легальной копии программного продукта.

Появление высоконадежных преобразователей биометрия-код [1] и биометрических нечетких хэш-функций [2] позволяет разработать новые и модифицировать классические методы защиты исполняемого кода программного обеспечения.

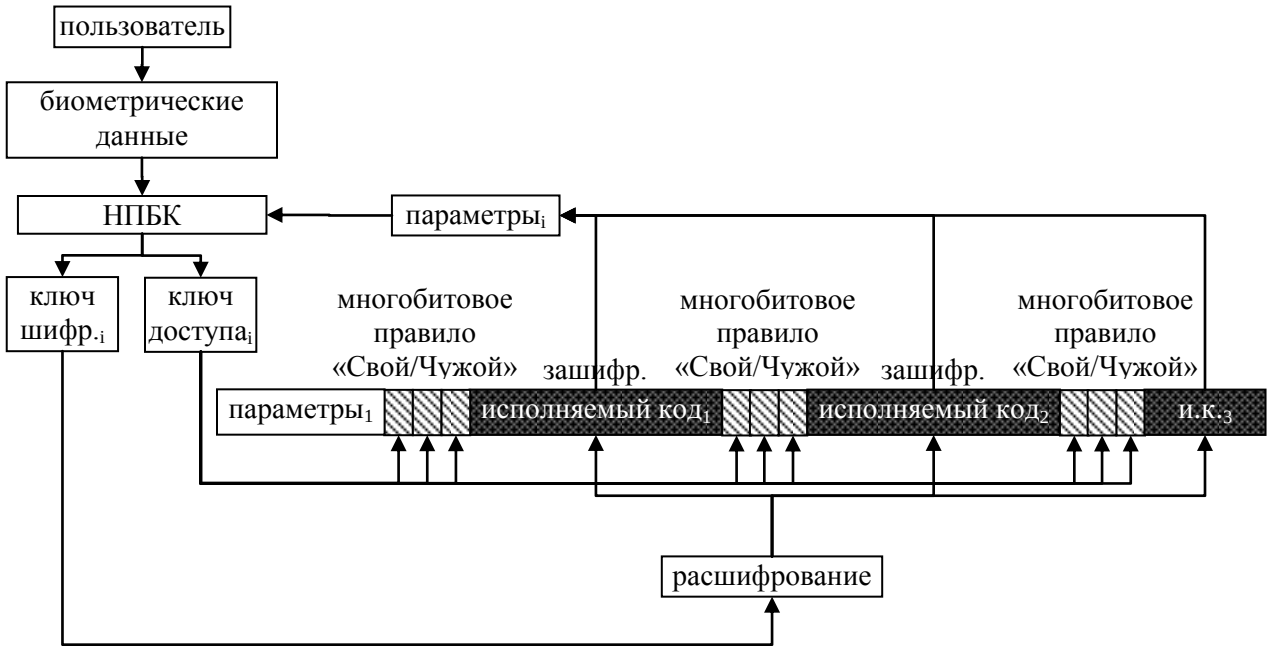

Рис 2. Схема биометрической защиты программ с ограничением доступа

На Рис.2 показана модифицированная схема защиты исполняемого кода, достигаемая совмещением процедур шифрования и высоконадежного преобразования биометрия-код. При использовании динамической биометрии пользователя риск компрометации ключа доступа значительно снижается, поскольку ни в программе, ни в рабочем окружении на ПЭВМ он не хранится. Для контроля легальности пользователя используется многобитовое решающее правило, которое трудно подменить, поскольку оно может быть реализовано как безусловное (индекс таблицы переходов, адрес вызова или адрес перехода, счетчик цикла и т.д.). Генерация параметров нейросетевого преобразователя биометрия-код (НПБК) производится во время продажи конкретному пользователю. Значит, биометрическая схема защиты программы также будет работать для третьей угрозы, поскольку отследить на основании взломанной копии злоумышленника, купившего копию программы и распространявшее программу нелегально также возможно.

Для обеспечения более высокого класса защиты исходных кодов от исследования предлагается использовать схему биометрического транслятора исполняемых кодов, показанную на Рис.3. Вместо зашифрованного исполняемого кода в этом случае модули программы хранят вектора параметров НПБК, а также таблицы исполняемых кодов и таблицы переходов. При предъявлении легальным пользователем своих биометрических данных на выходе НПБК вырабатываются правильные индексы инструкций и адресов, которые во время трансляции переводятся в исполняемые коды и адреса программы. Данная схема позволяет производителю генерировать полиморфные программы, а следовательно, в значительной мере затруднять их исследование и параллельное эмулирование. Все данные программы хранятся в открытом виде, поэтому использование «тяжелых» криптографических функции в этом варианте не понадобится.

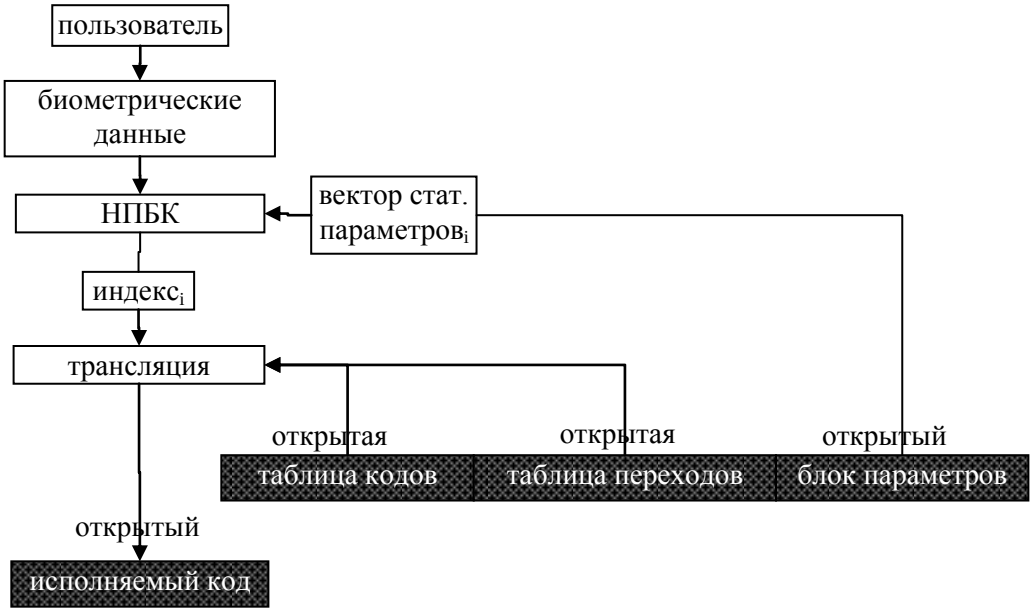

Рис 3. Схема биометрической защиты программ с трансляцией исполняемого кода

Особенности биометрических образов (избыточность), а также возможность с помощью НПБК регулировать вероятности ошибок 1-го и 2-го рода позволяют предложить новый метод защиты: динамическую биометрическую защиту программ с контролем вероятностей ошибок первого и второго рода. Схема биометрической защиты представлена на Рис 4.

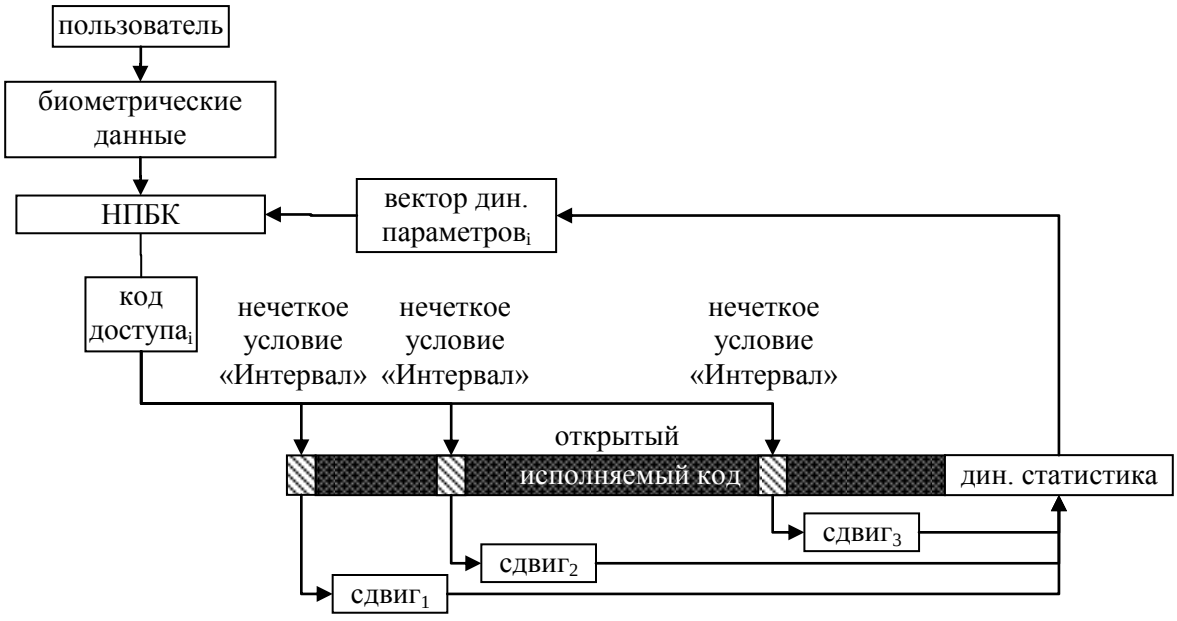

Рис 4. Схема динамической биометрической защиты программ с контролем вероятностей ошибок первого и второго рода

В предложенной схеме во время работы программы собирается динамическая статистика. Динамическая статистика представляет собой набор параметров с разной

степенью устойчивости, например, движения мышью, нажатие на кнопки клавиатуры, вызовы функций, время задержек, длительность циклов, хэш-значения, вырабатываемые на основе введенных биометрических данных и т.д. Отдельные параметры динамической статистики, вместе с биометрическими данными пользователя (также обладающими нестабильностью) подаются на вход НПБК, который вырабатывает код доступа. С помощью нечетких условий «Интервал» (проверка на вхождение в некоторый интервал), во-первых, принимается решение о продолжении работы с программой, а во вторых вычисляется некоторый динамический параметр сдвиг, изменяющий динамическую статистику. Параметр сдвиг может вычисляться, например, как разница между сгенерированным кодом доступа и некоторыми эталонным значением. Параметр сдвиг так изменяет динамическую статистику, что решение об отказе легальному пользователю или злоумышленнику принимается не на текущем шаге, а только через несколько шагов, что позволяет значительно затруднить пошаговую отладку программы. Обратный поиск точек, в которых была корректировка сдвига также затруднена, поэтому исследование программы, защищенной таким образом, в некоторых случаях может быть сопоставимо с написанием аналогичной.

Заключение

Таким образом, в настоящей работе предложены 3 метода биометрической защиты программного обеспечения, улучшающих известные классические методы. Теоретико-практическое исследование характеристик указанных методов планируется продолжить в следующих работах.

СПИСОК ЛИТЕРАТУРЫ

1. *Волчихин В.И., Иванов А.И., Фунтиков В.А.* Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации //-Пенза: Изд-во Пенз. гос. ун-та, 2005, 276с;
2. *Майоров А.В.* Нейросетевая хэш-функция //журнал «Нейрокомпьютеры. Разработка и применение», №6, 2009, ISSN 0869-5350, с.45.