Но для контроля искажений большей длины, а это присуще искажением искусственного характера, этот вид контроля применять нецелесообразно.

2. Контроль целостности информации в файлах позволяет вскрыть значительно меньшее, чем при предшествующем виде контроля, количество искажений, но ***наибольшей, максимальной при пофайловом контроле длины*** и потому ***этот вид контроля целесообразно применять при контроле целостности информации*** файлов, в случае необходимости такого контроля, например, целостности информации, ***которая дискретно оперативно изменяется.***

При контроле же процессов обмена информацией следует учесть следующее:

1. Методы блочно-группового контроля целостности информации, с их выше определенными особенностями, могут быть легко приспособленными для контроля процессов обмена без использования механизмов решающей обратной связи, что приведёт к повышению скорости обмена (длина блока должна отвечать длине сообщения, принятой в соответствующем протоколе. Это просто реализуется, например, в протоколе X.25).

2. Контроль целостности информации в блоках, длина которых превышает длину сообщения (контроль в файлах), разрешает применять принципы каскадных кодов, и обеспечивать целостность в условиях влияния то ли помех большой продолжительности (количество искажений превышает корректирующие свойства внутреннего кода), то ли продолжительных (в том же понимании) замираний сигналов.

Следует, кроме того, обратить внимание и на то, что вычисление контрольных признаков предложенными методами имеет все признаки, необходимые для хеш–функций и некоторых видов *цифровой подписи*, а следовательно могут в определенных случаях выполнять их функции.

Литература: 1. Нормативный документ Системы технической защиты информации "Общие положения про защиту информации в компьютерных системах от несанкционированного доступа" (НД ТЗИ 1.1 – 002 – 99). 2. Нормативный документ Системы технической защиты информации "Критерии оценки защищенности информации в компьютерных системах от НСД" (НД ТЗИ 2.5 – 004 – 99). 3. Нормативный документ Системы технической защиты информации "Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа" [НД ТЗИ 2.5.–005 –99]. 4. Василенко В. С., Короленко М. П. Целостность информации в автоматизированных системах. // Корпоративные системы. 1999. – № 3.– с. 52–57. 5. Василенко В. С., Курочкин С. Г. Использование метода помехоустойчивой криптографии в системах обработки кредитно-финансовой информации // Машинная обработка информации. Межведомственный научный сборник.– Вып. 60, 1997. – с. 169–174. 6. Будько М. М., Василенко В. С., Короленко М. П. Механізми контролю цілісності та її поновлення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, – К., 2000. – с. 130 – 139.

УДК 519.25

РЕАЛИЗАЦИЯ МЕХАНИЗМОВ ЗАЩИТЫ И АНАЛИЗА ОБРАЗНОГО ОПЕРАЦИОННОГО ЯДРА

Александр Манухин
Служба безопасности Украины

Анотація: **Показана можливість побудови образного операційного ядра на прикладах реалізації механізмів цілісності та автентичності даних.**
Summary: **There is shown possibility of building of figurative operating kernel on examples of realization of mechanisms of wholeness and authenticity of data.**
Ключові слова: **Конфіденційність, цілісність даних, операційна система, образ, функція хешування, кластер.**

I Введение

Относительно информации, как объекта исследования, технологические процессы (субъекты) выступают источником объекта, его потребителем или нарушителем, поскольку на нынешнем этапе развития технологий информационное окружение – это автоматизированные системы (АС) обработки данных. Собственно АС представляет собой совокупность взаимосвязанных организационно-технических компонентов:

- технических способов обработки и передачи динамических объектов (вычислительной техники и связи);
- статических объектов на различных носителях (массивов, наборов, баз данных);
- методов и алгоритмов обработки (программного обеспечения);
- персонала и пользователей системы.

Важность и значения объектов для тех или иных субъектов информационных отношений в условиях скрытого коммерческого, ведомственного и государственного интереса определить сложно. Разумеется, удовлетворение информационных потребностей находится в пропорциональной зависимости от условий и методов (способов) практической деятельности соответствующих субъектов. В связи с этим объекты, циркулирующие в АС, по рангу доступа бывают открытыми и с ограниченным доступом (конфиденциальными).

Информационная безопасность АС обеспечивается лишь в случае, когда для любых информационных ресурсов в системе поддерживается определенный уровень конфиденциальности (невозможности несанкционированного получения объектов), целостности (невозможности несанкционированной или случайной их модификации) и доступности (возможности за определенное время получить необходимый объект). Существует множество подходов относительно оценки концепции защиты объектов АС. В данной работе использована оценка с точки зрения доступа к нему, с градацией на 3 уровня: уровня носителей и способов взаимодействия с носителями, уровня представления и уровня содержания информации.

Методы реализации угроз информационной безопасности по уровням доступа представлены в табл. 1.

Таблица 1 – Методы реализации угроз информационной безопасности

Уровни доступа к объектам в АС	Угроза нарушения конфиденциальности	Угроза нарушения целостности объекта
Взаимодействия с носителями	- копирование субъектов; - перехват динамических объектов	- внесение изменений в субъекты и объекты
Представление объектов	- раскрытие представления объектов	- внесение искажений в представление объектов
Содержания объектов	- раскрытие содержания объектов (расшифровка)	- внедрение дезинформации (ложных объектов)

В данной работе ставится задача реализации наиболее критичных элементов ядра операционной системы: механизмов разграничения доступа и саморазвития.

II Постановка задачи

Анализ индивидуальных признаков программно-аппаратной среды, в которой обрабатывается исполняемый объект, дает ему возможность проверить легальность копии (процесса, данных) и принять решение о характере дальнейшей обработки, что позволяет локализовать наиболее уязвимое место любой системы защиты. Действительно, сама задача защиты объектов по сути своей дихотомична, т. е. предполагает выбор одного из двух возможных вариантов: либо копия легальна, либо нет (реализуется машинной инструкцией условного перехода). Если в коде программы заменить эту инструкцию командой безусловного перехода, то объект всегда будет обрабатываться так, как если бы проверка легальности копии дала положительный результат. Таким образом, каким бы хитроумным не был алгоритм проверки, он легко нейтрализуется в точках дихотомического ветвления командами безусловного перехода (алгоритм принятия решения сфокусирован). Идея защиты объектов, предлагаемая в данной работе, предполагает реализацию алгоритма распределенного принятия решения посредством использования функциональных зависимостей: алгоритм субъекта описывается функцией, настроенной в резонанс с условиями легальности (расфокусированная обработка). Таким образом, основой первого выбранного механизма является создание (или использование) хеш-функции и алгоритма ее использования.

Реализация второго механизма подразумевает придание операционной системе элементов искусственного интеллекта в вопросах анализа и распознавания данных. Следовательно, основа этого механизма – алгоритм представления и классификации данных.

III Реализация механизмов хеширования и кластерного анализа

Несмотря на кажущееся различие в реализациях механизмов, автором предлагается решить их на основе единой методологии [1] представления объекта, используя ее диаметрально противоположные качества:

точности и общности.

Пусть имеется порционный байтовый информационный поток (объект), требующий операционной обработки. Порцию (квант) объекта представим сообщением, использующим правила естественных языков (семантика, формат). В качестве исходного материала построения обоих механизмов возьмем образ *m*,

$$m = \bigvee_a m_a ,$$

где m_a – гармоника *m* индекса *a*.

Реализация механизма хеширования объекта.

Основанием для контроля целостности выступает контрольная сумма (КС) файла (результат хеширования файла, MAC). Базой построения алгоритма является совпадение содержания страницы кодирования знакогенераторов ПЭВМ, где используется код ASCII (American Standard Code of Information Interchange) в 8-битовом варианте. Количество символов знакогенераторов кодирования ПЭВМ – 0...255.

Примем следующие обозначения.

File = (a_i), $i \in [1,...,I]$, $a \in [0,...,255]$ – типизированный файл, тип элементов файла – символ; количество упорядоченных элементов *I* (объем файла), a_i – это *i*-элемент файла с ASCII-кодом знакогенератора ПЭВМ, равным *a*.

$R_{[v\text{-}w]}$ – выделение 10-чных разрядов числа *R*, начиная с разряда *"v"* и заканчивая разрядом *"w"*, $w \geq v$.

$R_{(q)}$ – число в системе исчисления *q* (по умолчанию q=10 не пишется).

Для решения задачи используется действительная внутренняя форма представления числа *X* типа EXTENDED (см. рис. 1).

$s_{[0, 16]}$	$e_{[17\text{-}20]}$	$m_{[2\text{-}15]}$

Рисунок 1 – Внутренняя форма представления действительного числа: где *s* – знаковые разряды числа, *e* – экспоненциальная часть числа, *m* – мантисса числа.

Для выработки контрольной суммы формируются два числа: $X_{(10)}$, $Y_{(32)}$. Поскольку форма действительного числа имеет 19–20 десятичных знаков (15 чисел – мантисса числа, 4 – экспоненциальная часть и знаки мантиссы и экспоненциальной части), математическая формализация задачи имеет цель изготовления электронному документу *File* (через переменную *X)* такого $Y_{(32)}$, *File* $\rightarrow Y_{(32)}$, что:

$$X_{(10)} = X^*_{[5-15]} = \left(\sum_{a=0}^{255} m_a (2 \cdot a + 1)\right)_{[5-15]}, \qquad X_{(10)} \Rightarrow Y_{(32)}, \tag{1}$$

где $m_a = \gamma_i$,

$$\gamma_i = \begin{cases} 0.236 \cdot \dfrac{i}{0.618 \cdot I}, & \textit{если} \quad i \leq 0.618 \cdot I. \\ 0.236 \cdot \dfrac{(I - i + 1)}{(I - 0.618 \cdot I + 1)}, & \textit{иначе.} \end{cases}, \tag{2}$$

Здесь символ "⇒" представляет собой оператор перевода в иные системы исчисления, что использует стандартные правила упаковки.

Полная контрольная сумма образа *X** содержит в себе объемную и модифицирующую составляющие; (1) выделяет последнюю, потому данная реализация использует точностную характеристику (качество) объекта.

Технология использования выработанного хеша подобна алгоритму цифровой подписи и использует полную контрольную сумму образа объекта.

Шаг 1. Формирование КС, *X**. Добавление КС к объекту.

Шаг 2. Предсказание КС нового объекта, $(X^*)'$. Данная процедура непротиворечива и использует свойство линейной составляющей КС [2].

Шаг 3. Повторять шаги 1–2 до тех пор, пока $Y_{(32)}$ нового объекта не будет равна $(X^*)'_{[5\text{-}15]}$.

Шаги 1–3 используются для наложения КС на объект. Алгоритм аутентификации объекта при сличении хеша полностью подобен процедуре сличения электронной подписи.

Реализация механизма самоорганизации субъекта.

Рассматриваемый механизм использует непосредственно образ *m*. Поскольку исследуемые объекты в общем случае представляют собой как разнородные, так и однотипные данные (первоначальную однородность, кластер), множество объектов интерпретируется множеством взаимно пересекающихся областей, каждая из которых представляет собой совокупность объектов одной однородности. Целью анализа выступает анализ взаимосвязей кластеров.

Расположив центры кластеров в пространстве объектов, изучив объемы кластерных перекрытий и динамику использования одного кластера множеством разнородных объектов, можно создать триангуляционную самоорганизующуюся систему. Следовательно, ключевой процедурой построения пространства файлов, упорядоченного с точки зрения того или иного целевого признака, является процедура анализа неоднородности. Листинг процедуры анализа однородности (центральный фрагмент) на метаязыке MathCAD представлен на рис. 2.

```
i2 ← cluster + 1
i2 ← 1  if  i2 > class
while  tbl_i2 ≠ 1
    i2 ← i2 + 1
    i2 ← 1  if  i2 > class
    i2 ← 1  if  i2 ≥ class  if  tbl_i2 ≠ 1
r01 ← READPRN(concat(concat(f_, num2str(cluster)), ".prn" ))
for  j1 ∈ 0.. higth
  f01_j1 ← r01_0,j1
rM0 ← supsmooth (v, f01)
rM0 ← (rM0 − min(rM0)) / max(rM0)
n_ ← 1
while  i2 ≠ cluster
    if  tbl_i2 = 1
        n_ ← n_ + 1
        r01 ← READPRN(concat(concat(f_, num2str(cluster)), ".prn" ))
        for  j1 ∈ 0.. a
          f01_j1 ← r01_0,j1
        rM1 ← supsmooth (v, f01)
        rM0 ← (rM0 − min(rM0)) / max(rM0)
        rM0 ← rM0 + (rM1 − rM0) · n_^(−1/step)
    i2 ← i2 + 1
    i2 ← 1  if  i2 > class
```

Рисунок 2 – Листинг процедуры анализа однородности объекта

Технология кластерного анализа представляет собой прохождение следующих шагов.

Шаг 1. Ввод классификации объектов. В качестве таковой могут быть внешние атрибуты объектов (файловые расширения, сигнатуры формата и т. п.). Впоследствии классификация сдвигается в сторону внутренних атрибутов (семантики файловых элементов).

Шаг 2. Формирование образа объекта. Вначале образ формируется согласно (1) – (2) для алогичных объектов, впоследствии алгоритм формирования образа изменяется согласно анализируемым запросам

(например, смысловая обработка текстов, графики и т. п.).

Шаг 3. Сглаживание образа одного класса. Поскольку образ представляет собой объединение гармоник, его можно функционально описать огибающей. Процесс сглаживания огибающей должен быть регулируемым. Вначале возможно применить сглаживание Фридмана [3], впоследствии качество сглаживания доводится до нуля (нет сглаживания).

Шаг 4. Повторять шаги 2–3 для объектов одного класса.

Шаг 5. Анализ неоднородности образов одного класса. Регулируемым параметром в данной процедуре является порог близости сглаженных образов огибающих друг к другу. На выходе шага имеем множество кластеров, составляющих данный класс.

Шаг 6. Повторять шаги 2–5 для всех классов выдвинутой классификации.

Шаг 7. Формирование кластерного пространства. Построение пространства начинается с вычисления центрального кластера и упорядочивания кластеров в порядке убывания их взаимосвязи. На этом этапе выбираются 3 любых базовых кластера и относительно них, в полярной системе координат, пересчитывается пространственная формула (метод триангуляции). Использование локальных пространственных формул имеет свойство самоорганизации: при позиционировании триангуляционных лучей в пустоте принимается решение о новом классе классификации (для шага 8).

Шаг 8. Изменение или уточнение классификации. В первом случае повторяются шаги 1–7 для нового классообразования. Во втором случае, в зависимости от целевого признака анализа, корректируются элементы шага 2, 3, 5 (для каждого шага они описаны как изменяющиеся впоследствии). Повторять шаги 1–8 до тех пор, пока качество сглаживания не равно нулю (шаг 3).

Поскольку процедура механизма самоорганизации предполагает использование сглаживающих методов, данная реализация использует качество общности объекта.

IV Выводы

В работе рассмотрена возможность реализации механизмов разграничения доступа и саморазвития операционной системы, построенной на принципах распознавания образов. Показано, что данные механизмы используют диаметрально противоположные характеристики самого образа, точности и общности. Остальные механизмы, не рассмотренные в материале статьи, располагаются в пределах данного диапазона характеристик. Временные рамки описанных механизмов зависят от вычислительных ресурсов субъектов.

Литература: 1. Шелест М. Є., Манухін О. В. Основи побудови автоматизованої системи оперативного аналізу інформації у телекомунікаційних мережах // Спеціальні телекомунікаційні системи та захист інформації, вип. № 1. – К.: СБУ, 2001. – с. 77–83. 2. Розробка технології обліку файлів на об'єктах обчислювальної техніки: Звіт про НДР (заключний) / Військовий інститут НТУУ "КПІ". – № держреєстрації 0101U00798. – К., 2001. – 80 с. 3. Friedman J. H. A variable span scatterplot smoother // Laboratory for Computational Statistics, Stanford University Technical Report, 1984, № 5.

УДК 681.3

ВОЗМОЖНОСТЬ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ В КРИПТОПРОТОКОЛАХ, ОСНОВАННЫХ НА СВОЙСТВАХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Владислав Мухачев, Михаил Шелест
Служба безопасности Украины

Анотація: **Показано можливість впровадження прихованих каналів передачі інформації у цифровий підпис та протокол пересилки ключів, що побудовані на властивостях еліптичних кривих.**
Summary: **There is shown the possibility of embedding subliminal channels in digital signatures and key transport mechanisms based on elliptic curves.**
Ключові слова: **Прихований канал, стеганографія, цифровий підпис, криптопротокол, еліптична крива, кофактор.**

I Введение

В настоящее время для передачи данных по каналам связи общего пользования все большее применение находят стеганографические методы защиты информации, т. е. методы, основанные на принципах