УДК 519.25

# УРОВНЕВЫЙ АНАЛИЗ ИНФОРМАЦИИ В СИСТЕМЕ ОЦЕНКИ ЕЕ ЦЕЛОСТНОСТИ И ДОСТОВЕРНОСТИ

***Александр Манухин, Татьяна Ковальчук*, Вадим Томчук***
*Военный институт НТУУ "КПИ",*НИЦ "ТЕЗИС" НТУУ "КПИ"*

*Анотація:* **Розглядається проблема аналізу цілісності та достовірності інформації, що транслюється, на бінарному та логічному рівнях в контексті комплексних систем її захисту.**

*Summary:* **Considering problem of analysis safe and authentic information, what transmitting in the binary and logically levels, in a context complex protection systems of the information.**

*Ключові слова:* **Системи цілісності та достовірності інформації, коректуючі коди, електронний цифровий підпис, інформаційний конфлікт.**

## Введение

После поля и вещества информация представляет собой третий вид существования материи. Жизненный цикл ее трансформаций предполагает, что информация добывается, обрабатывается, хранится, охраняется, используется, транслируется, расхищается и уничтожается. В зависимости от условий она может выступать сырьем, продуктом, товаром и, как следствие, превращаться в деньги. Следовательно, информация, имеющая определенные стоимость (важность), цену и значение может представлять интерес для определенных потребителей – юридических и физических лиц во всех сферах общественной деятельности (субъекты исследования). В свою очередь это означает, что если объект не выдается добровольно и безвозмездно, если он не продается по приемлемой цене, то всегда будет иметь место стремление к его хищению. Таким образом, применение информационных технологий, требующих в определенных случаях сохранения конфиденциальности содержания объекта, обуславливает внедрение комплексной системы защиты информации (КСЗИ), что включает в себя способы контроля целостности и достоверности информационных потоков (СЦДИ).

Следует различать два уровня существования объекта – структурный и логический. Первый служит его материальной основой в виде лексико-грамматических языковых структур, второй – носитель интерпретирующей составляющей события у субъекта. Назовем первый уровень низким, второй – высоким и рассмотрим механизмы естественного (или искусственного) воздействия на объект с точки зрения его целостности и достоверности.

## II Низкий уровень трансляции объекта

Материальной основой структурного уровня объекта $M$ является его бинарное представление $2^n$-возможными кодовыми комбинациями, $M \Rightarrow V$. Ошибки трансляции для данного уровня возникают из-за врожденных или приобретенных дефектов носителя объекта, качества каналов связи, неисправностей электронного и электромеханического оборудования. Наиболее реальный способ обеспечения достоверности объекта – применение корректирующих кодов, служащих для обнаружения и коррекции ошибок.

В настоящее время разработано сравнительно большое количество корректирующих кодов, основанных на различных разделах математики: теории групп, коммутативной алгебры, теории конечных полей. Возможности обнаружения и коррекции ошибок повышаются при увеличении избыточности кода, однако, одновременно усложняются алгоритмы кодирования и декодирования. Для обеспечения высокой достоверности трансляции объекта при относительно простой технике кодирования и декодирования


*ISBN 966-622-022-9*
*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.*

разработаны циклические коды (циклическим называется код, который с любым своим вектором содержит также и его циклический сдвиг; следовательно, циклический сдвиг любого вектора является кодовым вектором), $M \Rightarrow Q(x)$. Они допускают компактное математическое описание и по своей структуре идеально приспособлены к реализации в современных технических устройствах.

Удобным алгебраическим средством для описания циклических сдвигов векторов являются многочлены. Вектору $a = (a_0, a_1, a_2, .., a_{n-1})$ поставим в соответствие многочлен $a(x) = a_0 + a_1 x + .. + a_{n-1} x^{n-1}$, в котором коэффициенты совпадают с соответствующими координатами вектора. Тогда циклическому сдвигу вектора $a$ соответствует многочлен $a'(x) = a_{n-1} + a_0 x + a_1 x^2 + ... + a_{n-1} x^n$. В общем случае,

$$a'(x) = xa(x) - a_{n-1}(x^n - 1). \tag{1}$$

Положим $x^n = 1$, тогда

$$a'(x) = xa(x). \tag{2}$$

Выражение (2) показывает, что циклический сдвиг любого вектора получается умножением многочлена, соответствующего этому вектору, на $x$, с умножением степеней по $\mathrm{mod}\, 2$:

$$x^k x^m = x^r, \quad r \equiv (k+m)(\mathrm{mod}\, 2), \quad 0 \le r < n.$$

Отметим, что умножение многочленов подчиняется коммутативному, ассоциативному и дистрибутивному законам алгебры логики. Поэтому множество всех многочленов $G(x), Q(x) \in G(x)$, степени не более $n$ образует относительно указанных операций кольцо. Из этого следует, что код объекта $V$ является циклическим только тогда, когда $V$ является идеалом в кольце $G$. Если $V$ идеал, то для каждого кодового многочлена $a(x) \in V$ имеем $a'(x) \in V$. В [1] доказана теорема представления, согласно которой во всяком идеале $V$ кольца $G$ существует фиксированный многочлен $g(x)$, которому кратен всякий многочлен идеала $V$. Отсюда, любой многочлен $a(x) \in V$ можно представить произведением фиксированного многочлена $g(x) \in V$ и некоторого подходящего многочлена $S(x) \in V$:

$$a(x) = g(x) \cdot S(x), \tag{3}$$

где $g(x)$ – порождающий многочлен идеала $V$ или циклического кода.

Следовательно, если известен $g(x)$, то известны и все кодовые многочлены. Число их равно произведению всевозможных комбинаций произвольного многочлена $S(x)$ степени не более $n$ на порождающий многочлен $g(x)$.

Процесс коррекции ошибки состоит в следующем. Принятая кодовая комбинация объекта делится на порождающий многочлен $g(x)$. Подсчитывается вес остатка $w$ (количество единиц). Если $w \le g$, то принятая кодовая комбинация складывается с остатком по $\mathrm{mod}\, 2$. Полученная комбинация считается исправленной. Если $w \ge g$, то производится циклический сдвиг влево на один разряд с последующим делением на $g(x)$ и снова проверка веса остатка. Операция повторяется до тех пор, пока не будет получено значение $w \le g$. Затем складывается последнее делимое с последним остатком и производится такое же количество сдвигов вправо, после которых комбинация соответствует переданной.

*ISBN 966-622-022-9*

Построение циклических кодов представляется в виде:

$$\frac{Q(x)x^r}{g(x)} = C(x) + \frac{P(x)}{g(x)}, \qquad (4)$$

где $Q(x)$ – кодовая комбинация объекта, частное $C(x)$ степени $r$ и остаток $P(x)$ степени $r-1$.

Техническая реализация (на линейных рекуррентных регистрах) циклических кодов по (4) предполагает детерминированное расположение символов во всех комбинациях, т. е. сначала расположены $k$ информационных, а затем $n-k$ контрольных символов объекта.

**II Средний уровень трансляции объекта**

Средний уровень трансляции объекта (с точки зрения СЦДИ) рассматривается при анализе граничных условий уровней его существования. Кодовое представление объекта (низкий уровень) имеет аппаратную поддержку выявления и коррекции ошибок, но не затрагивает логику объекта. Факт существования объекта (высокий уровень) передается языковыми средствами в форме электронных сообщений. Это обстоятельство и позволяет рассмотреть промежуточный уровень (средний) трансляции объектов, переданных по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации разнообразного назначения. Ошибки трансляции для данного уровня имеют, в основном, искусственную природу и приводят к искажению факта существования объекта. Действенное решение СЦДИ на среднем уровне – использование процедуры электронной цифровой подписи (ЭЦП). Эта ситуация аналогична ссылке на авторитетность источника объекта.

Стандарт ЭЦП [2] принят и введен в действие постановлением Госстандарта Украины № 640 от 21. 10. 97. Он устанавливает процедуры выработки и проверки ЭЦП сообщений (документов) на базе асимметрического криптографического алгоритма с применением функции хеширования (ДСТУ 34.311-95 и ГОСТ 28147-89). Только внедрение системы ЭЦП обеспечивает защиту объектов от подделки и искажения.

Цифровая подпись, которая составляется из двух целых чисел, представленных в виде слов в алфавите $\beta = \{0,1\}$, вычисляется с помощью определенного набора правил, изложенных в стандарте. Числа $p, q, a$, являющиеся параметрами системы, должны быть выбраны (выработаны) по процедуре стандарта [2] и не являются секретными. Конкретный набор их значений может быть общим для группы пользователей. Целое число $k, 0 < k < q$, генерируемое в процедуре подписи сообщения, секретное, и должно быть уничтожено сразу после изготовления подписи. Оно снимается с физического датчика случайных чисел или вырабатывается псевдослучайным методом с использованием секретных параметров. Процесс СЦДИ содержит в себе этапы выработки и проверки подписи (соответственно отправителем и адресатом). Отправитель направляет адресату цифровую последовательность символов, что составляет с бинарным представлением объекта и присоединенной к нему ЭЦП 512-битный вид $< r' >_{256} || < s >_{256}$:

$$r' = (a^k \pmod p) \pmod q, \quad s = (x \cdot r' + k \cdot h(M)) \pmod q, \qquad (5)$$

где $h(M)$ – значение функции хеширования объекта $M$, $x$ – секретный ключ пользователя для формирования подписи, $0 < x < g$.

Получатель должен проверить аутентичность сообщения и аутентичность ЭЦП (5), предпринимая ряд вычислений при наличии открытого ключа отправителя $y$:


*ISBN 966-622-022-9*
*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.*

$$(a^{s(h(M_1))^{q-2}(\mathrm{mod}\ q)(\mathrm{mod}\ q)} y^{(q-r`)(h(M_1))^{q-2}(\mathrm{mod}\ q)(\mathrm{mod}\ q)}(\mathrm{mod}\ p))(\mathrm{mod}\ q). \qquad (6)$$

Стандарт [2] предусматривает программную и аппаратную реализацию по (5)–(6).

## III Высокий уровень трансляции объекта

Рассматривая СЦДИ, отметим, что если на низком и среднем уровнях трансляции объекта выделялся преимущественно аспект целостности, то на высоком уровне – аспект ее достоверности. Высокий (логический) уровень трансляции объекта предполагает констатацию факта события по шкале “информация-дезинформация” и определенные субъекты будут сдвигать рейтинг объекта по данной шкале согласно собственным интересам [3].

Дезинформационный компонент достаточно часто используется для решения проблем в области информационных конфликтов, причем основа его должна быть информационной (т. е. дезинформация становится информацией, когда подается в контексте правды). Это положение вытекает из субъективных закономерностей интерпретации факта события. По объекту (на высоком, логическом, уровне – факту) можно построить различные интерпретации:

Символ 1 Символ 2
↑ ↑
Интерпретация 1 Интерпретация 2
└ Факт ┘

Этому способствует то обстоятельство, что субъект не в состоянии самостоятельно оценивать множество происходящих событий и за него необходимую интерпретацию делает авторитет в нужном ему контексте. На государственном уровне в роли интерпретатора выступают средства массовой информации (СМИ), заполняющие информационное пространство и подающие факты вместе с интерпретацией (лишь особая мыслительная операция позволяет отделить одно от другого). Таким образом, можно говорить о том, что трансляция объектов на высоком уровне способствует кристаллизации общественного мнения, поскольку более достоверная (или более ожидаемая социумом) информация имеет больше шансов быть транслируемой. Иными словами, процесс трансляции объектов одновременно формирует сами объекты.

Механизм передачи данных на логическом уровне затрагивает стандартные информационные цепочки в виде следующих наборов компонент:

Источник → Сообщение → Канал → Аудитория

В свою очередь, дезинформационная цепочка будет строиться на подмене одного из этих компонентов (или нескольких) псевдокомпонентом. При этом следует учесть, что успешность этой кампании определяется дефицитом объекта у субъекта. Рассмотрим структуры воздействия дезинформационного контекста на субъект.

В первом случае происходит порождение объекта от иного источника (оригинальный источник скрыт от аудитории). Это факт ссылки на “авторитетный” источник:

Источник 1
↓
Источник 2 → Сообщение → Канал → Аудитория

Второй случай комментируется как возможность подмены объектов в результате дефицита информации:

*ISBN 966-622-022-9*
*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.*

Сообщение 1

↓

Источник → Сообщение 2 → Канал → Аудитория

Третий вариант иллюстрируют подделку (“адаптацию”) канала трансляции объекта для субъекта:

Канал 1

↓

Источник → Сообщение → Канал 2 → Аудитория

Четвертый вариант – вариант “псевдоутечки” информации.

Аудитория 1

↓

Источник → Сообщение → Канал → Аудитория 2

Рассмотренные схемы позволяют лишь качественно оценивать степень воздействия объекта в нужном контексте на субъект. На практике применяются комбинационные схемы.

**Выводы**

Предложенный анализ некоторых особенностей и структуры информации как объекта исследования определяет один из вариантов изучения ее функций. На данном этапе развития электронно-вычислительной техники особое внимание обращается как на целостность информации, так и на контроль использования своих прав (по отношению к предмету информации) потребителями. Рассмотрение природы появления различных дезинформационных элементов позволит в дальнейшем правильно разбить эту проблему на основные составляющие, что, в свою очередь, позволит более корректно определить пути ее решения.

В статье рассмотрены стандартные тракты трансляции объектов и их первичный анализ в контексте дальнейшего изучения и решения проблемы безопасности их передачи, что позволяет сделать следующие выводы:

1. Информационная безопасность в общей системе национальной безопасности занимает особое место. С учетом темпов информатизации и развития информационных технологий, широкого внедрения таких технологий в производство, оборону, защиту прав, науку, образование – информационная безопасность является элементом всех составляющих национальной безопасности государства. В этой связи эта проблема все больше приобретает самостоятельное общественное значение. В то же самое время система внешних и внутренних угроз информационной безопасности носит комплексный характер и осуществление этих угроз имеет целью нанесение ущерба в политической, экономической, социальной, военной, экологической и научно-технической сферах. Ключевым элементом КСЗИ является система целостности и достоверности информации. Базовая роль данной системы определяется тем, что она является узловым моментом принятия решения относительно применения мер защиты. Эффективность СЦДИ достигается механизмами ее воздействия на самом элементарном уровне представления объекта.

2. Объект рассмотрения статьи представляет собой композицию структурного и логического уровней интерпретации. Структурный (нижний) уровень объекта служит для переноса его стандартными языковыми средствами и в электронном виде затрагивает его


*ISBN 966-622-022-9*
*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.*

бинарное представление. Логический (высокий) уровень объекта является носителем его смысловой насыщенности (факта). Собственно СЦДИ затрагивают разные аспекты своего инструментария по отношению к этим интерпретационным уровням – целостности на низком и достоверности на высоком уровнях.

3. Инструментарий СЦДИ позволяет на низком уровне выявлять и корректировать ошибки, на среднем (граничном) – только их выявлять. Особенности субъективного восприятия объекта позволяют полностью нивелировать степень достоверности факта объекта посредством подмены его контекста.

4. Анализируя объективно-субъективный континуум, можно говорить об определенных законах воздействия на субъект (при наличии детерминированного объекта), а именно:

- различимости: механизмы воздействия средствами низкого и среднего уровня на объект субъектом различимы, потенциально ожидаемы и, по большей части, прогнозируемы; механизмы воздействия высокого уровня субъективно неразличимы, что позволяет осуществить тонкую коррекцию факта (в сравнении с грубой на нижних уровнях);
- многонаправленности: интерпретационное восприятие объекта субъектом восприимчиво как к официальному (информационному), так и неофициальному (дезинформационному) каналам трансляции объектов;
- активной роли субъекта: в информационном мире процесс трансляции объектов одновременно формирует сами объекты;
- многослойности: объект содержит в себе не только факт, но и его интерпретацию, поэтому заимствование факта с иным объектом несет в себе и иную интерпретацию, что в подавляющем большинстве случаев не воспринимается субъектом; объект формируется как источником, так и потребителем;
- информационного усиления: искривление информационного пространства достигается за счет значимости объекта, а удержание внимания со стороны субъекта возможно только при качественной мотивации.

Методология анализа достоверности объекта, предложенная в статье, позволяет комплексно подойти к оценке контекста любых информационных событий, электронных документов и отрезков известных форматов различных потоков данных глобальной информационной сети.

*Литература: 1. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ / Под. ред. Р. Л. Добрушина, С. И. Самойленко. – М.: Мир, 1976. 2. ДСТУ 34.310-95. 3. Почепцов Г. Информация и дезинформация // Досье секретных служб, № 3, 2001*

**УДК 681.31**

# ВАРІАНТ ПІДВИЩЕННЯ ШВИДКОСТІ ФОРМУВАННЯ ОЗНАК ЦІЛІСНОСТІ В МЕХАНІЗМАХ КОНТРОЛЮ ЦІЛІСНОСТІ

***Микола Будько, Вячеслав Василенко, Руслан Балидін***
*ВАТ "КП ОТІ", м. Київ*

*Анотація*: **Запропоновано варіант організації контролю цілісності та варіант прискорення формування ознак цілісності при модифікації інформаційного об'єкту.**

*Summary:* **The article presents variant of organization of the control of integrity and variant of acceleration of formation of integrity attributes at updating information object.**

*Ключові слова*: **Захист інформації, цілісність інформації, контроль, імітостійкість, ознака цілісності.**

## Вступ