можна визначити суб'єктивним шляхом за допомогою методу експертних оцінок. Далі задачу можна розділити на дві підзадачі [3].

Перша з них полягає у визначенні системи, що забезпечує найвищу ефективність $Q_э=f[\varphi_1(x), \varphi_2(x), \varphi_3(x) \ldots. \varphi_{m-1}(x)]=max,$ при допустимому значенні вартості $C \le C_{max}$.

Результатом рішення ***другої*** задачі має бути система, що забезпечує $C=C_{min}$ при $Q_э=f[\varphi_1(x), \varphi_2(x), \varphi_3(x) \ldots. \varphi_{m-1}(x)] \ge Q_{min}$

Таким чином, складні системи, до яких можна віднести систему управління інфокомунікаціями, можна оцінити за допомогою декількох показників якості. Для вибору оптимального варіанту побудови системи управління необхідно функціонування системи представити у вигляді математичної моделі, яка характеризується набором показників якості і критеріїв оптимальності. Різноманітність і складність розв'язання задачі багатокритерійної оптимізації передбачає в якості додаткової інформації наявність даних про відносну важливість цих критеріїв. При цьому в якості узагальненого критерію оптимальності можуть використовуватися: *адитивний* критерій оптимальності, *мультиплікативний* критерій оптимальності, *узагальнений* логічний критерій оптимальності, *середньоступеневий* узагальнений критерій оптимальності.

Література

1. Батищев Д.И. Методы оптимального проектирования / Д.И. Батищев. – М.: Радио и связь, 1984. – 247с.

2. Стеклов В. К. Системный метод оптимального проектирования интеллектуальной сети / В.К. Стеклов, Л.Н. Беркман // Зв'язок. – 1998. – №4. – С.43-49.

3. Штойер Р. Многокритериальная оптимизация / Р. Штойер. – М.: Радио и связь, 1992.

УДК 62-55:681.515

Ткаленко О.Н., к.т.н. *(Государст. унив-т информационно-коммуникационных технологий)*

ПРИМЕНЕНИЕ В AQM СИСТЕМАХ НЕЧЕТКОГО РЕГУЛЯТОРА С ИЗМЕРЕНИЕМ ДЛИНЫ ОЧЕРЕДИ И УРОВНЯ ИСПОЛЬЗОВАНИЯ БУФЕРА

Ткаленко О.М. Застосування в AQM системах нечіткого регулятора з вимірюванням довжини черги та рівня використання буфера. У даній роботі запропоновано декілька основаних на нечіткій логіці ефективних алгоритмів управління перевантаженнями в мережах TCP/IP, головна перевага яких не у використанні механізму відкидання пакетів RED, а в обчисленні втрати пакетів згідно попередньо сконфігурованій нечіткій логіці з використанням довжини черги та рівня використання буферу.

Ключові слова: МЕРЕЖА TCP/IP, ПЕРЕВАНТАЖЕННЯ, АКТИВНЕ УПРАВЛІННЯ ЧЕРГОЮ, AQM, НЕЧІТКИЙ РЕГУЛЯТОР

Ткаленко О.Н. Применение в AQM системах нечеткого регулятора с измерением длины очереди и уровня использования буфера. В данной работе предложено несколько основанных на нечеткой логике эффективных алгоритмов управления перегрузками в сетях TCP/IP, главное преимущество которых не в использовании механизма отбрасывания пакетов RED, а в вычислении потери пакетов согласно предварительно сконфигурированной нечеткой логике с использованием длины очереди и уровня использования буфера.

Ключевые слова: СЕТЬ TCP/IP, ПЕРЕГРУЗКА, АКТИВНОЕ УПРАВЛЕНИЕ ОЧЕРЕДЬЮ, AQM, НЕЧЕТКИЙ РЕГУЛЯТОР

Tkalenko O.M. Appling in AQM systems Fuzzy Controller with measuring the queue length and buffer usage ratio. In this work proposed a few primary of fuzzy logic efficacious algoritms of control of the overloadings in networks TCP/IP, the main advantage wich is not in using packet-dropping RED, but in detecting the loss packet mechanism according to preceding configurated fuzzy logic with using the queue length and butter usage ratio.

Keywords: NETWORK TCP/IP, OVERLOADING, ACTIVE QUEUE MANAGEMENT, AQM, FUZZY-CONTROLLER

Введение. Предложено несколько эффективных нечетких алгоритмов управления перегрузками, основанных на нечеткой логике, которые используют преимущества нечеткой

логики при работе с недостоверными событиями. Главное преимущество этих новых алгоритмов управления перегрузками состоит в том, что они не используют механизма отбрасывания пакетов RED, а вычисляют потери пакетов согласно предварительно сконфигурированной нечеткой логике с использованием длины очереди и уровня использования буфера. Основная идея алгоритма AQM состоит в слежении за уровнем перегрузок на сети и сообщении источникам пакетов об этом так, чтобы они уменьшали свою скорость передачи. В условиях, когда источники в сети конкурируют за полосу пропускания и буферное пространство не зная о текущем состоянии ресурсов и не имея информации друг о друге, перегрузки возникают, когда требуемая полоса пропускания превышает доступную емкость связи. Это приводит к резкому ухудшению характеристик сети, поскольку увеличиваются потери пакетов и уменьшается эффективность использования связи. Чтобы избежать этих проблем, необходима некоторая организация и управление трафиком.

Отметим, что RED-алгоритм [1] управляет очередью, случайно отбрасывая пакеты с увеличивающейся вероятностью при увеличении средней длины очереди от нижнего предела до верхнего предела. Одна из главных целей RED-алгоритма состоит в использовании комбинации усредненной длины очереди (которая учитывает всплески трафика) и раннего уведомления о перегрузках (которое уменьшает среднюю длину очереди), чтобы одновременно достичь низкой средней задержки очереди и высокой пропускной способности. Моделирование и опыт эксплуатации показывают, что RED-алгоритм достаточно успешен в этом отношении. Но средняя задержка очереди RED чувствительна к трафику (средняя длина очереди меняется от уровня перегрузок) и настройки параметров. Учитывая, что задержка является главным компонентом качества обслуживания, операторы хотели бы иметь хотя бы грубую априорную оценку средней задержки в маршрутизаторах, но для этого необходимо постоянно настраивать параметры RED-алгоритма для приспособления к текущим условиям трафика.

Традиционные методы не могут решить эту проблему с удовлетворительным качеством, в то время как нечеткая логика обеспечивает неаналитический подход к проектированию динамических и быстрых схем управления. Поскольку нечеткое управление может хорошо приспособиться к динамической окружающей среде без точной модели, нечеткая логика становится широко применяемой в TCP/IP сетях [2].

Исследование AQM системы с нечетким регулятором. В работе [3] предложено эффективное AQM, основанное на нечеткой логике, которое не использует механизм отбрасывания пакетов RED, а вычисляет потери пакетов согласно входной длине очереди и уровню использования буфера, что позволяет улучшить характеристики маршрутизаторов в IP-сетях при динамической окружающей среде. Основным элементом системы AQM является нечеткий регулятор (НР) – рис.1. Нечеткий регулятор (фаззи-регулятор, fuzzy-controller) включает три основных блока – блок фаззи-фикации (fuzzyfication), блок формирования логического решения (inference) и блок дефаззификации (defuzzyfication) [4, 5].

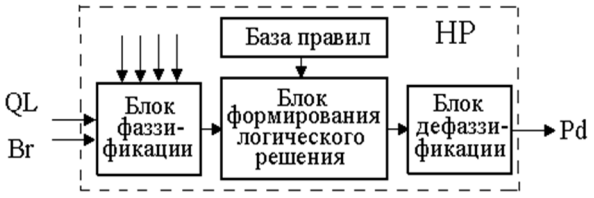

Рис. 1. Структура нечеткого регулятора

НР имеет два входа: длина очереди (queue length – QL) и уровень использования буфера (buffer usage ratio – Br), и один выход – вероятность отбрасывания пакетов (packet-dropping probability – Pd). Регулятор вычисляет вероятность отбрасывания пакетов, согласно длине очереди, текущему уровню использования буфера и набору нечетких правил.

Лингвистические правила обычно определяют следующим образом:

Правило 1: ЕСЛИ QL=A1 И Br=B1, ТО Pd=C1;
Правило 2: ЕСЛИ QL=A2 И Br=B2, ТО Pd=C2;
……;
Правило к: ЕСЛИ QL=Ак И Br=Вк=2, ТО Pd=Ск.

В качестве функций принадлежности используются симметричные треугольные и трапециевидные функции принадлежности. Длина очереди классифицирована в три лингвистических переменных: QL ={Короткая, Средняя, Длинная}, где «Короткая» означает, что длина очереди находится в нормальном состоянии, «Средняя» означает, что длина очереди находится в состоянии предотвращения перегрузки, «Длинная», означает, что длина очереди находится в состоянии перегрузки.

Рис. 2,а показывает функции принадлежности переменной «длина очереди».

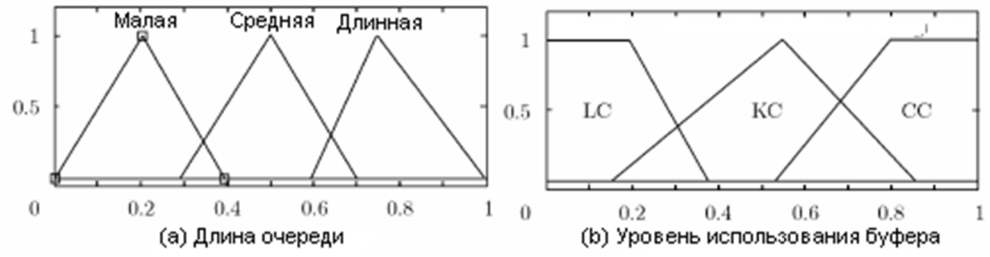

Рис. 2. Функции принадлежности входных переменных

Уровень использования буфера также классифицирован в три лингвистических переменных: Br = {Менее перегружен, Довольно перегружен, Сильно перегружен}, где «Менее перегружен», сокращенно LC, означает, что уровень использования буфера находится в нормальном состоянии; «Довольно перегружен», сокращенно KC, означает, что уровень использования буфера находится в состоянии предотвращения перегрузок; «Сильно перегружен», сокращенно CC, означает, что уровень использования буфера находится на уровне перегрузок. Рис.2,б показывает функции принадлежности переменной ”уровень использования буфера”.

Рис. 3 показывает функции принадлежности выходной переменной «вероятность отбрасывания пакетов». Вероятность отбрасывания пакетов классифицирована в пять лингвистических переменных: Pd ={Очень Низкая, Низкая, Средняя, Высокая, Очень Высокая}, или Pd = {OH, H, C, B, OB}.

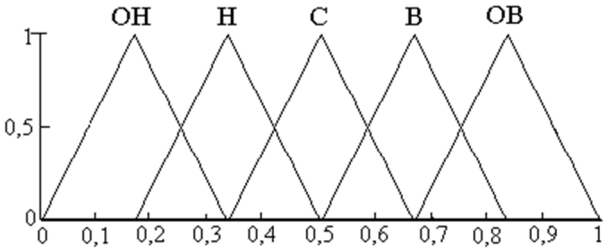

Рис. 3. Функции принадлежности переменной «вероятность отбрасывания пакетов»

В табл.1 записаны нечеткие правила, используемые для данного регулятора. На рис.4 представлены полные связи между входными и выходной переменными HP (поверхность отклика).

Нечеткие правила для регулятора **Табл. 1**

Длина очереди QL	Уровень использования буфера Br		
	Нормальное состояние	Предотвращение перегрузок	Перегрузки
Короткая	OH	OH	C
Средняя	OH	H	B
Длинная	H	C	OB

Когда пакет прибывает, измеряются текущие значения длины очереди QL и уровень использования буфера Br и вычисляется вероятность отбрасывания пакетов Pd согласно двум входам и нечетким правилам нечеткого управления перегрузками.

Оценка работы алгоритма на нечеткой логике для AQM в IP-сети. На рис.5 приведена архитектура нечеткого алгоритма AQM, которая содержит классифицирующую модель – КМ, модели отбрасывания пакетов – МОП и модель нечеткого регулятора – НР. ЛС – линия связи. Отношение входа-выхода выражено набором лингвистических правил.

Когда длина очереди короткая и уровень использования буфера низкий (буфер мало перегружен), то вероятность отбрасывания пакетов низкая. когда длина очереди большая и уровень использования буфера высокий (буфер сильно перегружен), то вероятность отбрасывания пакетов высокая. В этой системе, алгоритм может соответственно приспособить вероятность отбрасывания пакетов посредством "обучения".

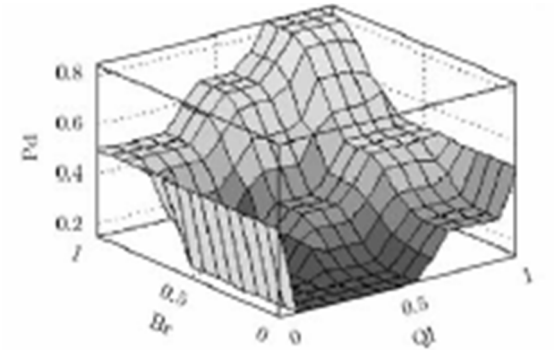

Рис. 4. Поверхность отклика HP

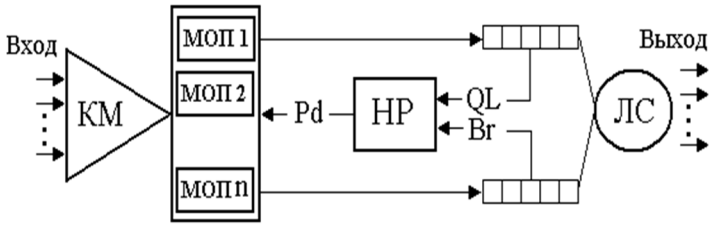

Рис. 5. Архитектура нечеткого алгоритма AQM

Оценка работы алгоритма на нечеткой логике для AQM в IP-сети выполнена путем моделирования на платформе ns2 при использовании гантелевидной топологии (см. рис. 6).

Предложенная схема была проверена в IP-сети, где есть только одна перегруженная связь от маршрутизатора Router1 до Router2.

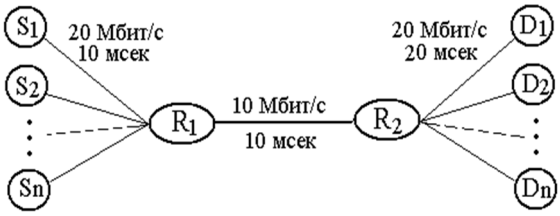

Рис. 6. Топология моделирования

Полоса пропускания связи (Link bandwidth) 10 Мбит/с, задержка связи (Link delay) составляет 10 мсек. Размер буфера – 300 пакетов, а ожидаемая длина очереди – 100 пакетов. Кроме того, во всех источниках активирована поддержка ECN (Explicit Congestion Notification). Продолжительность моделирования равна 100 секунд.

При моделировании предложенный алгоритм AQM с нечетким регулятором сравнивается с алгоритмами RED и PI-регулятора (PI-controller). Они внедрены между Router1 и Router2 при той же окружающей среде на сети. При моделировании RED используется "мягкая" версия и некоторые параметры по умолчанию в симуляторе ns2, min-th и max-th установлены в 20% и 80%, соответственно. Для PI-регулятора также используются параметры по умолчанию в ns2.

В первом эксперименте выбрано 100 (рис.7,a) и 600 (рис.7,b) соединений TCP. Когда $n = 100$, при использовании нечеткого, RED и PI алгоритмов длина очереди никогда не достигала размера буфера. Для трех алгоритмов это не трудно достигнуть при определенном состоянии сети и настройке параметров. Как следует из рис.7,a длина очереди RED больше, чем у нечеткого и PI алгоритмов. Длина очереди PI немного колеблется, в то время как длина очереди нечеткого алгоритма более устойчива и меньше.

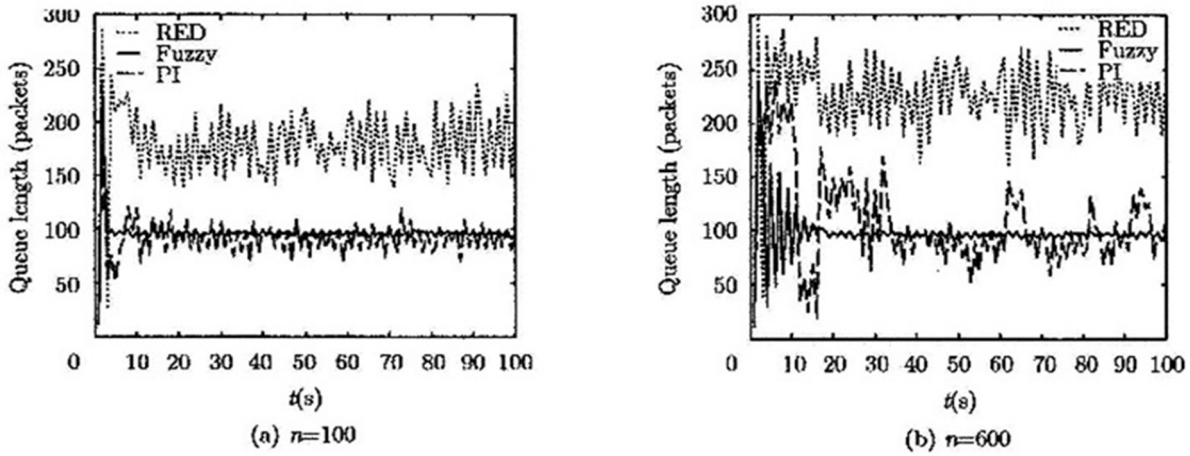

Рис. 7. Длина очереди для различных TCP соединений

Когда $n = 600$, длина очереди RED непостоянна, и колебание очереди, управляемой RED, больше, чем для нечеткого алгоритма. Для RED требуется некоторое время, чтобы среагировать на увеличивающееся число соединений, и длина очереди RED значительно

увеличивается и становится нестабильной. Длина очереди PI стабильна, но реакция является медленной. Предложенный нечеткий алгоритм поддерживает наименьшую длину очереди при увеличении числа соединений TCP. нечеткий алгоритм использует превосходство нечеткой логики при работе с неопределенными событиями. Даже без точной модели, он может хорошо использовать ресурс буфера, чтобы избежать колебаний, вызванных всплесками соединений. Он обеспечивает устойчивую длину очереди при переменной окружающей сети.

Результаты моделирования демонстрируют, что нечеткий алгоритм ускоряет скорость ответа AQM, даже если размер буфера маршрутизатора малый. PI требует довольно много времени, чтобы стабилизировать всплеск соединений. При переменной окружающей сети, для PI очень трудно поддерживать длину очереди на низком уровне. Характеристики AQM чувствительны к соединениям и ухудшаются с увеличением количества соединений.

Предложенный нечеткий алгоритм поддерживает более короткую и более устойчивую длину очереди, даже если число соединений быстро увеличивается. Он может быстро управлять длиной очереди, чтобы поддерживать её близкой к ожидаемому значению, даже при переменности окружающей среды.

Во втором эксперименте оценивается пропускная способность трех алгоритмов. Результаты эксперимента представлены на рис. 8.

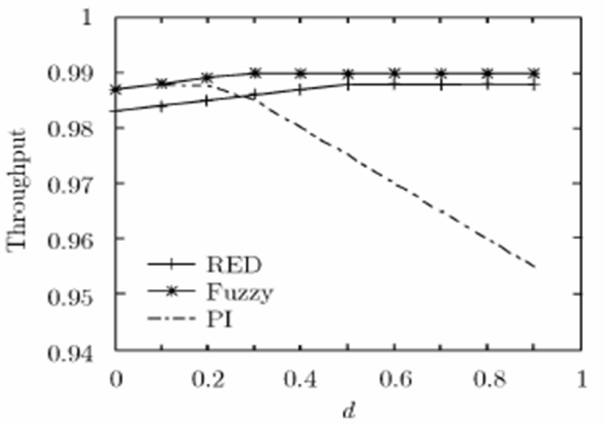

Рис. 8. Пропускная способность

Объектом этого эксперимента является исследование влияния UDP-потоков. Каждый UDP-поток является потоком ВКЛ/ВЫКЛ, плотность потока UDP изменяется от 0.1 до 0.9. Предложенный нечеткий алгоритм имеет более высокую пропускную способность, даже если вводятся потоки UDP. Он имеет более короткую и более устойчивую длину очереди, когда трафик изменяется. В той же самой окружающей сети, RED и PI имеют более высокую длину очереди и более низкую пропускную способность, RED имеет лучшие свойства, чем PI. При использовании алгоритма PI, UDP-потоки вызывают большие колебания, его пропускная способность быстро снижается, использование сети на уровне 95%. Для нечеткого алгоритма использование сети 99%. Использование связи для нечеткого алгоритма значительно больше, чем для RED и PI. Это может защитить поток TCP от потока UDP. Таким образом, характеристики предложенного нечеткого алгоритма превосходят PI и RED алгоритмы. Главное преимущество этого алгоритма состоит в том, что длина очереди может быть сохранена устойчивой при переменной окружающей сети без трудности в настройке параметров.

Вывод. Результаты теоретического анализа и моделирования в модели сети (Network simulator-ns2) показывают, что предложенные алгоритмы достигают большей пропускной способности и более устойчивой длины очереди, чем традиционные схемы. Они действительно улучшают способности маршрутизаторов (Routers) в управлении перегрузками в IP-сети.

Литература

1. Chrysostomou C., Pitsillides A., Polycarpou M., Sekercioglu A., “Fuzzy Logic Controlled RED: Congestion Control in TCP/IP Differentiated Services Networks”, Special Issue on "The Management of Uncertainty in Computing Applications" in Soft Computing Journal - a Fusion of Foundations, Methodologies and Applications, Vol 8, Number 2, pp. 79 - 92, December 2003.

2. Chrysostomou C., Pitsillides A., Hadjipollas G., Polycarpou M., Sekercioglu A."Fuzzy Logic Congestion Control in TCP/IP Best-effort Networks", Australian Telecommunications Networks and Applications Conference (Atnac 2003), Melbourne, Australia, 8–10 December 2003.

3. Liu Weiyan, Zhang Shunyi, Zhang Mu, Liu Tao. "A Fuzzy-Logic Control Algorithm for Active Queue Management in IP Networks". - Journal of Electronics (China), Vol.25, No.1, January 2008.

4. Гостев В.И. Нечеткие регуляторы в системах автоматического управления / В.И. Гостев. – К.: Издательство "Радіоаматор", 2008. – 972 с.

5. Гостев В.И. Проектирование нечетких регуляторов для систем автоматического управления / В.И. Гостев. – Спб.: Бхв-Петербург, 2011. – 416 с.

УДК 511.216

Яремчук Ю.Є., *к.т.н.* (*Вінницький національний технічний університет*)

МАТЕМАТИЧНИЙ АПАРАТ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ПОБУДОВИ КРИПТОГРАФІЧНИХ МЕТОДІВ З ВІДКРИТИМ КЛЮЧЕМ

Яремчук Ю.Є. Математичний апарат рекурентних послідовностей для побудови криптографічних методів з відкритим ключем. В роботі розглянуто рекурентну U_k-послідовність, для якої встановлено аналітичні залежності безпосереднього обчислення елементу послідовності, а також обчислення елементів U_k-послідовності тільки на основі елементів V_k^+-послідовності. Створений математичний апарат може стати основою для побудови криптографічних методів з відкритим ключем.

Ключові слова: КРИПТОГРАФІЯ, МАТЕМАТИЧНИЙ АПАРАТ, РЕКУРЕНТНА ПОСЛІДОВНІСТЬ, V_k^+-ПОСЛІДОВНІСТЬ,, V_k^--ПОСЛІДОВНІСТЬ

Яремчук Ю.Е. Математический аппарат рекуррентных последовательностей для построения криптографических методов с открытым ключом. В работе рассмотрено рекуррентную U_k-последовательность, для которой установлены аналитические зависимости непосредственного вычисления элемента последовательности, а также вычисления элементов U_k-последовательности только на основе элементов V_k^+ - последовательности. Созданный математический аппарат может стать основой для построения криптографических методов с открытым ключом.

Ключевые слова: КРИПТОГРАФИЯ, МАТЕМАТИЧЕСКИЙ АППАРАТ, РЕКУРРЕНТНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, V_k^+-ПОСЛЕДОВАТЕЛЬНОСТЬ, V_k^--ПОСЛЕДОВАТЕЛЬНОСТЬ,

Iaremchuk Iu.Ie. Mathematical apparatus of recurrent sequences for constructing cryptographic techniques with public key. We consider recursive U_k-sequence for which an analytical dependence of direct computation element sequences and computing elements U_k-order only on the basis of elements V_k^+-sequence. Created mathematical tools can be the basis for the construction of cryptographic techniques with public key.

Keywords: CRYPTOGRAPHY, MATHEMATICAL APPARATUS, RECURRENT SEQUENCE, V_k^+-SEQUENCE, V_k^--SEQUENCE

Вступ. Рекурентні послідовності в загальному вигляді породжується таким співвідношенням $u_n = a_1 u_{n-1} + a_2 u_{n-2} + ... + a_k u_{n-k}$, де $a_1, a_2, ..., \tilde{a}_k$ коефіцієнти, $\tilde{k}$ порядок послідовності, виходячи з початкових елементів $u_0, u_1, ..., u_k$ [1].

Складність обчислення елементів такої послідовності залежить від кількості ненульових коефіцієнтів $a_1, a_2, ..., a_k$ та від порядку k рекурентного співвідношення.