ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

DOI 10.54398/2074-1707_2022_1_85
УДК 004.052

ПОВЫШЕНИЕ СКОРОСТИ ОБНАРУЖЕНИЯ ОШИБОК ПРИ ФОРМИРОВАНИИ ЦЕПОЧЕК БЛОКОВ ДАННЫХ НА ОСНОВЕ АНАЛИЗА ЧИСЛА СОВПАДЕНИЙ ХЕШЕЙ [1]

Статья поступила в редакцию 29.11.2021, в окончательном варианте – 31.01.2022.

Таныгин Максим Олегович, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б,
кандидат технических наук, доцент, заведующий кафедрой информационной безопасности, ORCID: 0000-0002-4099-1414, e-mail: tanygin@yandex.ru
Кулешова Елена Александровна, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б,
преподаватель кафедры программной инженерии, ORCID: 0000-0002-8270-564X, e-mail: lena.kuleshova.94@mail.ru
Митрофанов Алексей Васильевич, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б,
аспирант кафедры информационной безопасности, ORCID: 0000-0001-7200-6418, e-mail: mitro3000@rambler.ru
Гладилина Елена Юрьевна, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б,
студент, e-mail: elena.gladilina@inbox.ru

В статье исследуется практическая реализация системы контроля целостности и аутентичности информации на основе CBC-кодов с целью повышения скорости обнаружения ошибок при формировании цепочек блоков данных. В рамках реализации схемы проверки блоков данных предлагается формировать древовидные структуры информационных блоков путём анализа атрибутов последних, при этом факт возникновения ошибки определяется на основе числа и длины ветвей в такой древовидной структуре. В статье предложен метод определения источника сообщений, который основан на анализе содержимого имитовставки и индекса сообщения в последовательности между двумя служебными сообщениями: стартовым, являющимся корнем древовидной структуры, и стоповым, которое должно быть последним сообщением в ветви. В основе исследования лежит математическая модель формирования древовидной структуры, на основании которой получены рекуррентные зависимости для вероятности формирования ветвей от корневого сообщения и вероятности формирования различных значений имитовставок сообщений этих ветвей. В работе показано, что существует взаимосвязь между числом ветвей древовидной структуры, порождаемых совпадениями значений атрибутов информационных блоков, и вероятностью ошибки при определении источника. На основе полученных оценок в работе сформулировано правило обработки ветвей древовидной структуры для сообщений ограниченной длины. Экспериментальные исследования показали, что применение данного правила позволит увеличить долю полезной информации, обрабатываемой приёмником, на 2–5 % за счёт снижения числа переспрашиваемых в результате обнаруженных ошибок аутентификации блоков данных.

Ключевые слова: передача данных, приёмник сообщений, система аутентификации, цепочки блоков данных, скорость обнаружения ошибок

INCREASING THE SPEED OF ERROR DETECTION WHEN FORMING CHAINS OF DATA BLOCKS BASED ON THE ANALYSIS OF THE NUMBER OF HASH MATCHES

The article was received by the editorial board on 29.11.2021, in the final version – 31.01.2022.

Tanygin Maxim O., Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, Head of the Department of Information Security, ORCID: 0000-0002-4099-1414, e-mail: tanygin@yandex.ru
Kuleshova Elena A., Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,
Lecturer at the Department of Software Engineering, ORCID: 0000-0002-8270-564X, e-mail: lena.kuleshova.94@mail.ru

[1] Исследование выполнено в рамках реализации внутриуниверситетского гранта по программе развития ЮЗГУ (ПРИОРИТЕТ-2030) № ПР2030/2021-27.

Mitrofanov Alexey V., Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,

Postgr. St. of the Department of Information Security, ORCID: 0000-0001-7200-6418, e-mail: mitro3000@rambler.ru

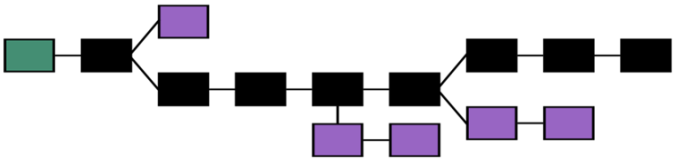
Gladilina Elena Yu., Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,

student, e-mail: elena.gladilina@inbox.ru

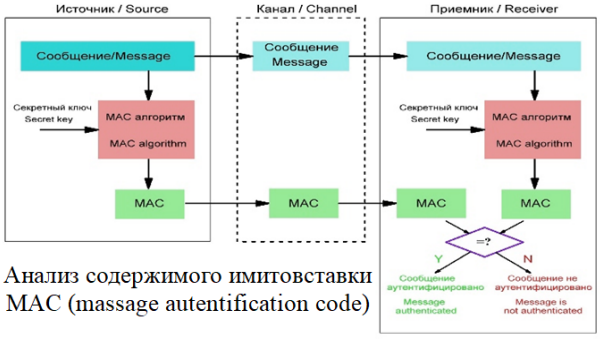
The article investigates the practical implementation of a system for monitoring the integrity and authenticity of information based on CBC codes in order to increase the speed of error detection when forming chains of data blocks. As part of the implementation of the scheme for checking data blocks, it is proposed to form tree-like structures of information blocks by analyzing the attributes of the latter, while the fact of an error is determined on the basis of the number and length of branches in such a tree-like structure. The article proposes a method for determining the source of messages, which is based on the analysis of the MAC content and the message index in the sequence between two service messages: start, which is the root of the tree structure, and stop, which should be the last message in the branch. The study is based on a mathematical model of the formation of a tree structure, on the basis of which recurrent dependencies for the probability of the formation of branches from the root message and the probability of the formation of different values of MAC messages of these branches are obtained. The paper shows that there is a relationship between the number of branches of the tree structure, generated by coincidences of the values of the attributes of information blocks, and the probability of error in determining the source. Based on the estimates obtained, a rule for processing branches of a tree structure for messages of limited length is formulated in the work. Experimental studies have shown that the application of this rule will increase the share of useful information processed by the receiver by 2–5 % by reducing the number of data blocks requested as a result of detected authentication errors.

Keywords: data transmission, message receiver, authentication system, data block chains, error detection rate

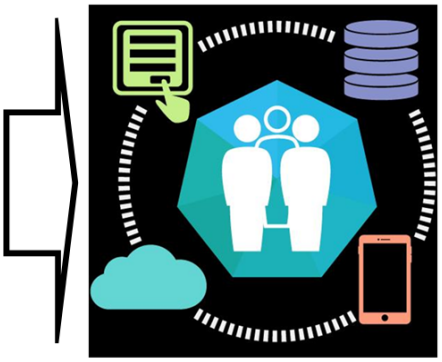
Graphical annotation (Графическая аннотация)



Формирование древовидной структуры информационных блоков
Formation of a tree structure of information blocks



Анализ содержимого имитовставки
MAC (massage autentification code)



Система контроля целостности
и аутентичности
Integrity and Authenticity
Control System

Введение. Широкое распространение автоматических систем управления технологическими процессами [1–3], формирование сетей, объединяющих в себя различные устройства мониторинга и управления техническими объектами [4, 5], влечёт за собой необходимость разработки специализированных протоколов передачи и обработки команд и данных. Особенности форматов данных и процесса их передачи, такие как временное разделение канала связи, передача данных в режиме широковещательных запросов [6, 7], вкупе с возросшими требованиями по обеспечению информационной безопасности таких систем [8, 9] обусловливает необходимость использования новых подходов к обеспечению аутентичности и целостности передаваемых и обрабатываемых данных. Использование ставших традиционными алгоритмов шифрования и помехоустойчивого кодирования не позволяет достичь требуемых показателей достоверности [10–13].

Кодирование передаваемых данных в режиме сцепления блоков является единственным средством повышения вероятности правильной аутентификации источника сообщений в условиях ограниченного размера поля имитовставки (англ. MAC – massage autentification code) [14, 15]. В то же время практическое применение такого подхода для выделения из общего потока команд

и данных сообщений от целевого источника порождает проблему обработки сложных структур [16]. Причиной этого является то, что при формировании структурированных последовательностей, в которых позиция каждого сообщения задана не напрямую индексом сообщения, а взаимным расположением относительно других сообщений (что позволяет обеспечить требуемую достоверность), в результате совпадения значений имитовставок различных сообщений вместо цепочки формируется сложная древовидная структура.

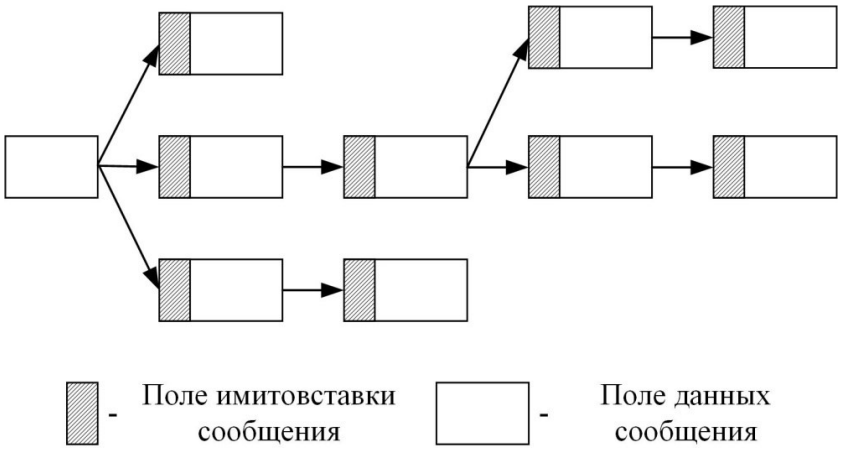


Рисунок 1 – Структура, формируемая в приемнике из-за совпадения значений имитовставок

В работах [17, 18] представлены оценки вероятности для числа и длины L ветвей в таких древовидных структурах, а также предложена математическая модель оценки достоверности процедуры аутентификации и её вычислительной сложности. Кроме того, различные варианты алгоритмов формирования древовидных структур показали, что количество операций сравнения имитовставок сообщений зависит от количества сформированных к текущему числу во внутренней памяти приёмника ветвей древовидной структуры [18]. Число таких сравнений непосредственно увеличивает вероятность возникновения коллизии, т. е. ситуации, при которой две или более ветви структуры удовлетворяют всем требованиям, предъявляемым к последовательности сообщений, чтобы быть ассоциированной с конкретным источником. Таким образом, число и размер ветвей в древовидной структуре оказываются связаны с достоверностью процедуры аутентификации источника, так как обе эти величины, как показано в [19], являются функцией вероятности случайного совпадения значений имитовставок, которая, в свою очередь, зависит от размера поля имитовставки в отдельном сообщении. Эта взаимосвязь является теоретической предпосылкой для обнаружения ошибок аутентификации не в результате анализа содержимого сообщений, входящих в ветви древовидной структуру, а на основе анализа числа таких цепочек на соответствующих этапах алгоритма.

Материалы и методы. Объектом исследования является метод определения источника сообщений, который основан на анализе содержимого имитовставки и индекса сообщения в последовательности между двумя служебными сообщениями: стартовым, являющимся корнем древовидной структуры, и стоповым, которое должно быть последним сообщением в ветви. В основе настоящего исследования лежит математическая модель формирования древовидной структуры, описанная в [19]. В ней, рассмотрев процесс формирования древовидной структуры, начиная с корня, получены рекуррентные зависимости для вероятности $p_r(k_r)$ формирования ровно k_r ветвей в позиции r от корневого сообщения и вероятности $p_r^{\mathrm{h}}\left(k_r^{\mathrm{h}}\right)$ формирования k_r^{h} различных значений имитовставок сообщений этих ветвей [16], которые вычисляются по (1):

$$p_r\left(k_r\right)=\sum_{l=k_r}^{|U|-n}\left[\frac{\left(\left(U-n\right)/n\right)^l\times e^{-\frac{(U-n)}{n}}}{l!}\times\sum_{k_{r-1}=1}^{|U|-n}p_{r-1}^{\mathrm{h}}\left(k_{r-1}^{\mathrm{h}}\right)\frac{\left(k_{r-1}^{\mathrm{h}}l2^{-H}\right)^l\times e^{-k_{r-1}^{\mathrm{h}}l2^{-H}}}{l!}\right],$$
$$p_r^{\mathrm{h}}\left(k_r^{\mathrm{h}}\right)=\sum_{l=k_r^{\mathrm{h}}}^{|U|-n}\left[p_r\left(l\right)\times\left(\left(2^{-H}\right)^{j-k_r^{\mathrm{h}}}\prod_{k=1}^{k_r^{\mathrm{h}}}\left(1-\left(k-1\right)2^{-H}\right)\right)\right]. \quad (1)$$

где U – общее число сообщений, обрабатываемых приёмником; H – размер поля имитовставки; k_r – число посторонних ветвей на расстоянии r от корня, n – длина цепочки сообщений.

В рассматриваемом подходе ошибка аутентификации источника блоков данных возникает, когда имитовставка, сформированная из какого-либо блока посторонней ветви древовидной структуры, совпадёт с имитовставкой соответствующего сообщения целевого источника. Вероятность этого определится по (2):

$$p_{\text{col}}(r)=\sum_{l=1}^{|U|-n}\left[p_r(l)\left(1-\left(1-2^{-H}\right)^l\right)\right], \tag{2}$$

где r – длина постороннней ветви.

Соответственно, функция зависимости вероятности возникновения ошибки от длины посторонней ветви, отсчитываемой от момента её отхода от основной ветви из сообщений целевого источника, рассчитывается по (3):

$$p\left(q_j\right)=C_{i-j}^{q_j}\left(p_{\text{col}}(j)\right)^{q_j}\left(1-p_{\text{col}}(j)\right)^{i-j-q_j},\ q_j=\overline{0\ldots} \tag{3}$$

где q_j – число возникших ошибок совпадения имитовставок; j – число сообщений в посторонней ветви, после которого возникла ошибка; i – позиция блока, от которого отходит посторонняя ветвь, в цепочке из n сообщений целевого источника.

Тогда вероятность возникновения ровно q ошибок совпадения значений имитовставок сообщений будет вычисляться по (4):

$$p^{\text{col}}(q)=\sum_{l=1}^{R[q]}\left(\prod_{k=1}^{l}p\left(q_k\right)\right),\ \sum_{k=1}^{l}q_k=q, \tag{4}$$

где $R[q]$ – число разбиений числа q на слагаемые q_k.

На основании рекуррентных формул (1) вероятность формирования в древовидной структуре q побочных ветвей, которые не привели к возникновению ошибки, определится как сумма произведений вероятностей по (5):

$$p^{\text{thr}}(q)=\sum_{l=1}^{R[q]}\left(\prod_{k=1}^{i-1}p_k\left(q_k\right)\right),\ \sum_{k=1}^{i-1}q_k=q. \tag{5}$$

Априорная вероятность формирования на определённом отдалении от корневого сообщения ровно q ветвей есть вероятность одновременного возникновения q' ошибок и q'' ветвей, ошибку не вызвавших. Исходя из того, что ошибка порождает дополнение посторонней ветви сообщениями целевого источника и удваивает число ветвей дерева, для q верно соотношение (6):

$$q=(q')^2+q''. \tag{6}$$

Априорная вероятность формирования двух ветвей в древовидной структуре вычисляется по (7):

$$p(2)=p^{\text{col}}(1)\cdot p^{\text{thr}}(0)+p^{\text{thr}}(2)p^{\text{col}}(0). \tag{7}$$

Для большего числа ветвей по (8):

$$\begin{aligned}
p(3)&=p^{\text{col}}(1)\cdot p^{\text{thr}}(1)+p^{\text{col}}(0)\cdot p^{\text{thr}}(3),\\
p(4)&=p^{\text{col}}(2)\cdot p^{\text{thr}}(0)+p^{\text{col}}(1)\cdot p^{\text{thr}}(2)+p^{\text{col}}(0)\cdot p^{\text{thr}}(4),\\
p(5)&=p^{\text{col}}(2)\cdot p^{\text{thr}}(1)+p^{\text{col}}(1)\cdot p^{\text{thr}}(3)+p^{\text{col}}(0)\cdot p^{\text{thr}}(5).
\end{aligned} \tag{8}$$

Определяем вероятности отсутствия ошибки аутентификации при разборе дерева сообщений $\overline{p}_i^{\text{col}}(0)$ при числе i сформировавшихся к определённому моменту ветвей дерева по (9):

$$\begin{aligned}
\overline{p}_2^{\text{col}}(0)&=\frac{p^{\text{thr}}(2)p^{\text{col}}(0)}{p^{\text{col}}(1)\cdot p^{\text{thr}}(0)+p^{\text{thr}}(2)p^{\text{col}}(0)},\\
\overline{p}_3^{\text{col}}(0)&=\frac{p^{\text{col}}(0)\cdot p^{\text{thr}}(3)}{p^{\text{col}}(1)\cdot p^{\text{thr}}(1)+p^{\text{col}}(0)\cdot p^{\text{thr}}(3)},\\
\overline{p}_4^{\text{col}}(0)&=\frac{p^{\text{col}}(0)\cdot p^{\text{thr}}(4)}{p^{\text{col}}(2)\cdot p^{\text{thr}}(0)+p^{\text{col}}(1)\cdot p^{\text{thr}}(2)+p^{\text{col}}(0)\cdot p^{\text{thr}}(4)},\\
\overline{p}_4^{\text{col}}(0)&=\frac{p^{\text{col}}(0)\cdot p^{\text{thr}}(4)}{p^{\text{col}}(2)\cdot p^{\text{thr}}(0)+p^{\text{col}}(1)\cdot p^{\text{thr}}(2)+p^{\text{col}}(0)\cdot p^{\text{thr}}(4)},\\
\overline{p}_5^{\text{col}}(0)&=\frac{p^{\text{col}}(0)\cdot p^{\text{thr}}(5)}{p^{\text{col}}(2)\cdot p^{\text{thr}}(1)+p^{\text{col}}(1)\cdot p^{\text{thr}}(3)+p^{\text{col}}(0)\cdot p^{\text{thr}}(5)}.
\end{aligned} \tag{9}$$

Большее число ветвей мы не рассматриваем, так как расчет по приведённым выше формулам (1) в различных диапазонах изменения параметров модели показал, что вероятность формирования 4-х и более отличающихся друг от друга ветвей древовидной структуры в каждой позиции $i = \overline{0\ldots}$ ветви сообщений целевого источника пренебрежимо мала (менее 10^{-3}).

Результаты и их обсуждение. На основании представленных выше формул получены зависимости апостериорной вероятности возникновения ошибки аутентификации от числа сформированных ветвей n^{thr} и длины ветви i, при которой происходит подсчёт числа ветвей (рис. 2). Отличительной особенностью данных графиков является то, что апостериорная вероятность отсутствия ошибок при четырёх побочных ветвях выше, чем при трёх. Причиной этого является то, что четыре ветви возникают тогда, когда есть одна ошибка, порождающая две ветви, и две ветви без ошибок, а вероятность формирования двух ветвей меньше, чем одной, как в случае с тремя ветвями.

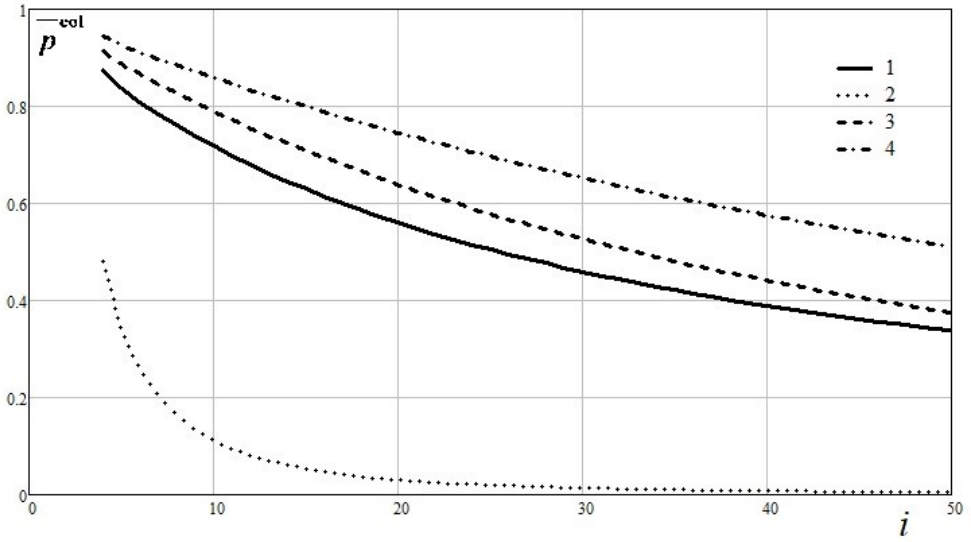


Рисунок 2 – График зависимости апостериорной вероятности $\overline{p}^{col}$ отсутствия ошибок аутентификации от числа сформированных посторонних ветвей n^{thr} в позиции i цепочки сообщений при U/n = 25: 1) $n^{th\,r}$= 2; 2) n^{thr} = 3; 3) $n^{th\,r}$= 4; 4) n^{thr} = 5

Кроме того, видно, что с ростом значения позиции сообщения априорная вероятность ошибки растёт. При i > 40 апостериорная вероятность ошибки при любом количестве посторонних ветвей достигает значений 60–80 %. Это позволяет в таком случае прекращать передачу сообщений от источника и фиксировать возникновение ошибки аутентификации при передаче всей цепочке. Актуальным этот результат является для случаев обмена данными последовательностями, содержащими большое число сообщений. Для исследования ситуаций с небольшой длиной анализируемых ветвей получена зависимость вероятности формирования побочной ветви длиной i от соотношения между длиной поля имитовставки и отношением между числом анализируемых сообщений и длиной цепочки (рис. 3, данные по оси ординат в логарифмическом масштабе).

Данная зависимость хорошо иллюстрирует тот факт, что вероятность формирования побочных ветвей формируемой приёмником древовидной структуры экспоненциально убывает с ростом длины такой ветви. Начиная с i = 5 ею можно пренебречь. Это позволяет сформулировать правило обработки древовидной структуры, заключающееся в следующем: если от какого-либо узла отходит ветвь длиной 6 и более элементов, то все остальные ветви, отходящие от данного узла и имеющие длину меньше 6, можно исключить из обработки. Если ветвей длиной 6 блоков данных обнаруживается более одной, то произошла ошибка формирования цепочки сообщений, при которой невозможно определить цепочку, выданную целевым источником. Дальнейшую передачу сообщений цепочки следует прекратить и перепослать все блоки данных, начиная с того, в котором была обнаружена ошибка.

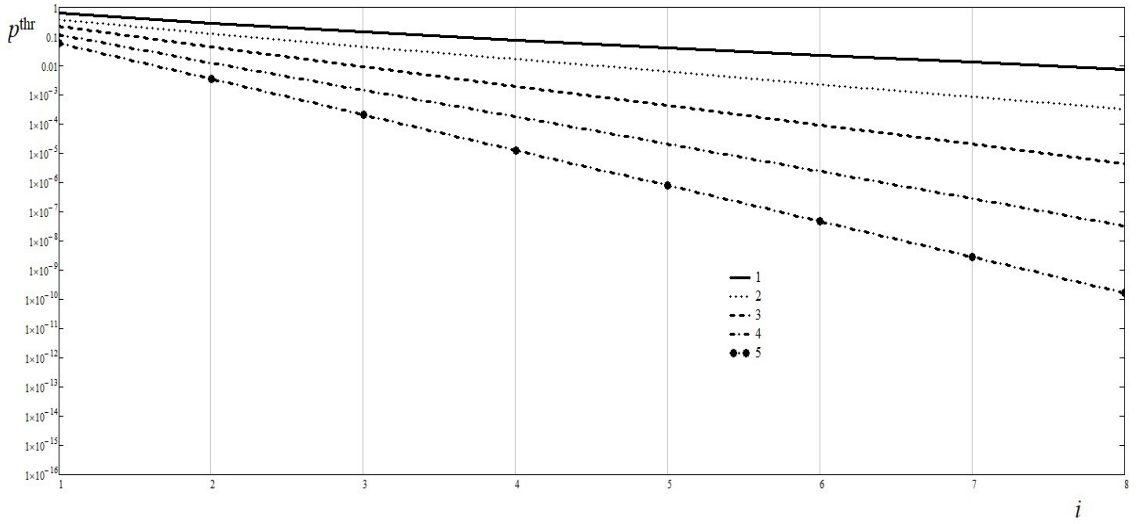


Рисунок 3 – График зависимости вероятности p^{thr} формирования побочной ветви длиной i от соотношения между длиной поля имитовставки и отношением U/n между числом анализируемых сообщений и длиной цепочки: 1) $U/n = 25$; 2) $U/n = 20$; 3) $U/n = 15$; 4) $U/n = 10$; 5) $U/n = 5$

Описанные действия позволят повысить долю полезной информации в общем объёме передаваемых между устройствами данных. Под полезной информацией мы понимаем содержимое всех полей информационного блока, кроме поля имитовставки, которая используется для аутентификации. Данный целевой параметр исчисляется по (10), учитывающей необходимость повторной передачи обработанной с ошибкой цепочки блоков данных [19].

$$K = \frac{L \cdot n \cdot \left(1 - P_{sc}\right)}{\left(L + H\right)\left(n + 2\right)}, \tag{10}$$

где L – длина поля полезной информации блока данных; P_{sc} – априорная вероятность возникновения ошибки аутентентификации источника при передаче цепочки блоков данных.

С учётом того, что P_{sc} при определённых целевых значениях длины поля имитовставки не превышает 0,1, то вероятностью возникновения ошибок в каждом из двух и более последовательно идущих циклов передачи данных можно пренебречь. Считаем, что средний номер блока в цепочке, в котором возникла ошибка $i_{col} \approx n/2$, и, с учётом уменьшения количества передаваемых блоков в следующем цикле передачи данных, формула (10) для доли полезной информации запишется в виде (11):

$$K' = \frac{L \cdot n}{\left(1 - p^{thr}\right)\sum_{i=0}^{\infty}\left[\left(\frac{n}{2^i} + 2\right)\left(1 - \prod_{j=1}^{\frac{n}{2^i}-1}\left(1 - p_{\text{col}}\left(j\right)\right)^{\frac{n}{2^i}-j}\right)^i\left(L + H + \right]\boldsymbol{log}_2\,\frac{n}{2^i}\left[+ 2\right)\right]}, \tag{11}$$

где p^{thr} – вероятность образования побочной ветви из 6 и более блоков.

Результат использования сформулированного выше правила обработки древовидной структуры заключается в увеличении доли полезной информации за счёт уменьшения объёма переспрашиваемой информации (рис. 4).

Из представленного на рисунке 4 графика видно, что в области максимума функции доли полезной информации она дополнительно повышается на 2–5 % в абсолютных значениях и до 30 % в относительных в зависимости от количества обрабатываемых приёмником блоков данных.

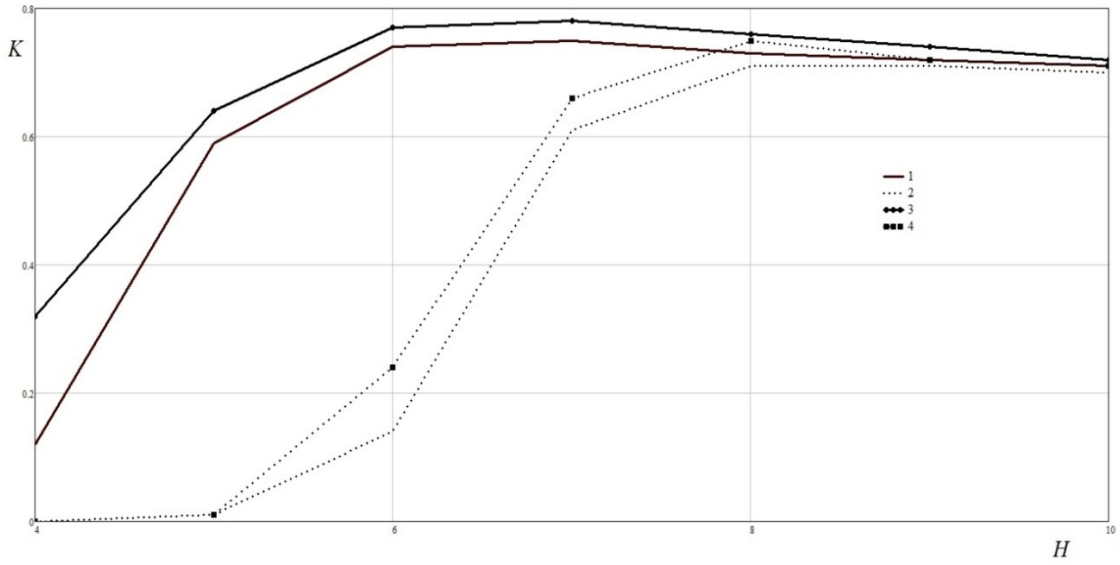


Рисунок 4 – Зависимость отношения K объёму полезной информации к общему объёму обрабатываемой приёмником информации от длины поля H при длине информационной части L = 40 битов, длине цепочки n = 30: 1) $|U|/n$ = 20, без использования правила обработки древовидной структуры; 2) $|U|/n$ = 20, с использованием правила обработки древовидной структуры; 3) $|U|/n$ = 130, без использования правила обработки древовидной структуры; 4) $|U|/n$ = 130, с использованием правила обработки древовидной структуры

Выводы. Результаты исследований показывают, что при использовании методов аутентификации для блоков, зашифрованных в режиме связывания, ошибки аутентификации возникают из-за совпадения содержимого кодов аутентификации сообщений (имитовставок). В результате вместо цепочки сообщений формируется древовидная структура, включающая как основную цепочку блоков, выданных целевым источником, так и некоторое количество посторонних, содержащих информационные блоки, выданные иными источниками. В рамках настоящей работы получены вероятностные оценки формирования посторонних цепочек как в случае правильного выполнения процедуры аутентификации, так и при возникновении ошибки. На основе полученных оценок сформулировано правило обработки ветвей древовидной структуры, подразумевающее исключение из обработки ветвей длиной менее 6. Для сообщений ограниченной длины применение данного правила позволяет увеличить долю полезной информации, обрабатываемой приёмником на 2–5 % за счёт снижения числа переспрашиваемых в результате обнаруженных ошибок аутентификации блоков данных.

Библиографический список

1. Sen, S. Profibus / S. Sen // Fieldbus and Networking in Process Automation. – 2021. – P. 119–144.
2. Sen, S. Modbus and Modbus Plus / S. Sen // Fieldbus and Networking in Process Automation. – 2021. – P. 145–156.
3. Hernández-Vázquez, H. Development of Virtual Router Machine for Modbus Open Connection / H. Hernández-Vázquez, I. Sanchez, F. Martell, J. Guzman, R. Ortiz // Recent Trends in Sustainable Engineering, Proceedings of the 2nd International Conference on Applied Science and Advanced Technology. – Budapest, Hungary, 2021. – P. 1–14.
4. Ondrej, S. ZigBee Technology and Device Design / S. Ondrej, B. Zdenek, F. Petr, H. Ondrej // International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06). – Morne, Mauritius, 2006. – P. 129–129.
5. Knapp, H. RFID systems optimisation through the use of a new RFID network planning algorithm to support the design of receiving gates / H. Knapp, G. Romagnoli // Journal of Intelligent Manufacturing. – 2021.
6. Moon, J. Covert Communications in Time Division Multiple Access Networks / J. Moon // The Journal of Korean Institute of Communications and Information Sciences. – 2021. – Vol. 46 (9). – P. 1407–1410.
7. Dua, A. Covert Communication using Address Resolution Protocol Broadcast Request Messages / A. Dua, V. Jindal, P. Bedi // 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). – Noida, India, 2021. – P. 1–6.
8. Borzenkova, S. Methodology for determining a set of measures to ensure information security in the automated process control system / S. Borzenkova, A. Sychugov // Journal of Physics: Conference Series. – 2020. – Vol. 1679. – P. 1–8.
9. Sviridov, A. The Concept of Information Security in the Process Control System / A. Sviridov, V. Bobkov, D. Bobrikov, A. Balashov // IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). – Saint Petersburg and Moscow, Russia, 2019. – P. 2162–2164.

10. Мальчуков, А. Н. Система автоматизированного проектирования кодеков помехоустойчивых кодов короткой длины / А. Н. Мальчуков, А. Н. Осокин // Известия Томского политехнического университета. – 2008. – Т. 312, № 5. – С. 70–75.

11. Мыцко, Е. А. Исследование алгоритмов вычисления контрольной суммы CRC8 в микропроцессорных системах при дефиците ресурсов / Е. А. Мыцко, А. Н. Мальчуков, С. Д. Иванов // Приборы и системы. Управление, контроль, диагностика. – 2018. – № 6. – С. 22–29.

12. Black, J. CBC MACs for arbitrary-length messages: The three-key constructions / J. Black, P. Rogaway // J. Cryptol. – 2015. – Vol. 18, № 2. – P. 111–131.

13. Liu, C. Implementation of DES Encryption Arithmetic based on FPGA / C. Liu, J. Ji, Z. Liu // AASRI Procedia. – 2013. – Vol. 5. – P. 209–213.

14. Stallings, W. NIST Block Cipher Modes of Operation for Confidentiality / W. Stallings // Cryptologia. – 2010. – № 34 (2). – P. 163–175.

15. Ben Othman, S. An efficient secure data aggregation scheme for wireless sensor networks / S. Ben Othman, H. Alzaid, A. Trad, H. Youssef // IISA 2013. – Piraeus, Greece, 2013. – P. 1–4.

16. Попов, А. Ю. Исследование вариантов реализации алгоритмов Крускала и Прима в вычислительной системе с многими потоками команд и одним потоком данных / А. Ю. Попов // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. – 2015. – № 11. – С. 505–527.

17. Таныгин, М. О. Сложность алгоритма определения источника данных / М. О. Таныгин, Х. Я. Алшаиа, А. В. Митрофанов // Труды МАИ. – 2021. – № 117. – С. 1–21.

18. Таныгин, М. О. Рекурсивный алгоритм формирования структурированных множеств информационных блоков для повышения скорости выполнения процедур определения их источника / М. О. Таныгин, О. Г. Добросердов, Х. Я. А. Алшаиа, В. П. Добрица // Известия Юго-Западного государственного университета. – 2021. – № 2. – С. 51–64.

19. Таныгин, М. О. Теоретические основы идентификации источников информации, передаваемой блоками ограниченного размера : монография / М. О. Таныгин. – Курск : ЗАО «Университетская книга», 2020. – 198 с.

References

1. Sen, S. Profibus. *Fieldbus and Networking in Process Automation*, 2021, pp. 119–144.

2. Sen, S. Modbus and Modbus Plus. *Fieldbus and Networking in Process Automation*, 2021, pp. 145–156.

3. Hernández-Vázquez, H., Sanchez, I., Martell, F., Guzman, J., Ortiz, R. Development of Virtual Router Machine for Modbus Open Connection. *Recent Trends in Sustainable Engineering, Proceedings of the 2nd International Conference on Applied Science and Advanced Technology*. Budapest, Hungary, 2021, pp.1–14.

4. Ondrej, S., Zdenek, B., Petr, F., Ondrej, H. ZigBee Technology and Device Design. *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*. Morne, Mauritius, 2006, pp. 129–129.

5. Knapp, H., Romagnoli, G. RFID systems optimisation through the use of a new RFID network planning algorithm to support the design of receiving gates. *Journal of Intelligent Manufacturing*, 2021.

6. Moon, J. Covert Communications in Time Division Multiple Access Networks. *The Journal of Korean Institute of Communications and Information Sciences*, 2021, vol. 46 (9), 2021, pp. 1407–1410

7. Dua, A., Jindal, V., Bedi, P. Covert Communication using Address Resolution Protocol Broadcast Request Messages. *9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. Noida, India, 2021, pp. 1–6.

8. Borzenkova, S. Sychugov, A. Methodology for determining a set of measures to ensure information security in the automated process control system. *Journal of Physics: Conference Series*, 2020, vol. 1679, pp. 1–8.

9. Sviridov, A., Bobkov, V., Bobrikov, D., Balashov, A. The Concept of Information Security in the Process Control System. *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. Saint Petersburg and Moscow, Russia, 2019, pp. 2162–2164.

10. Malchukov, A. N., Osokin, A. N. Sistema avtomatizirovannogo proyektirovaniya kodekov pomekhoustoychivykh kodov korotkoy dliny [A computer-aided design system for short-length error-correcting codes]. *Izvestiya Tomskogo politekhnicheskogo universiteta* [Bulletin of the Tomsk Polytechnic University], 2008, vol. 312, no. 5, pp. 70–75.

11. Mytsko, E. A., Malchukov, S. D. Issledovaniye algoritmov vychisleniy kontrolnoy summy CRC8 v mikroprotsessornykh sistemakh pri defitsite resursov [Investigation of algorithms for calculating the CRC8 checksum in microprocessor systems with a shortage of resources]. *Pribory i sistemy. Upravleniye, kontrol, diagnostika* [Devices and systems. Management, control, diagnostics], 2018, no. 6, pp. 22–29.

12. Black, J., Rogaway, P. CBC MACs for arbitrary-length messages: The three-key constructions. *J. Cryptol.*, 2015, vol. 18, no. 2, pp. 111–131.

13. Liu, C., Ji, J., Liu, Z. Implementation of DES Encryption Arithmetic based on FPGA. *AASRI Procedia*, 2013, vol. 5, pp. 209–213.

14. Stallings, W. NIST Block Cipher Modes of Operation for Confidentiality. *Cryptologia*, 2010, no. 34 (2), pp. 163–175.

15. Ben Othman, S., Alzaid, H., Trad, A., Youssef, H. An efficient secure data aggregation scheme for wireless sensor networks. *IISA 2013*. Piraeus, Greece, 2013, pp. 1–4.

16. Popov, A. Yu. Issledovanie variantov realizatsii algoritmov Kruskala i Prima v vychislitelnoy sisteme s mnogimi potokami komand i odnim potokom [Investigation of options for the implementation of the Kruskal and Prima algorithms in a computing system with many command streams and one data stream]. *Nauka i obrazovanie: nauchnoe izdanie MGTU im. N.E. Baumana* [Science and Education: scientific publication of MSTU im. N.E. Bauman], 2015, no. 11, pp. 505–527.

17. Tanygin, M. O., Alshaia, H. Ya., Mitrofanov A. V. Slozhnost algoritma opredeleniya istochnika dannykh [The complexity of the algorithm for determining the data source]. *Trudy MAI* [Proceedings of the MAI], 2021, no. 117, pp. 1–21.

18. Tanygin, M. O., Dobroserdov, O. G., Alshaia, H. Ya. A., Dobritsa, V. P. Rekursivnyy algoritm formirovaniya informatsionnykh blokov dlya povysheniya skorosti vypolneniya protsedur opredeleniya ikh istochnika [Recursive algorithm for the formation of structured sets of information blocks to increase the speed of execution of procedures for determining their source]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta* [Bulletin of the South-West State University], 2021, no. 2, pp. 51–64.

19. Tanygin, M. O. *Teoreticheskiye osnovy identifikatsii informatsii, peredavaemoy blokami ogranichennogo razmera : monografiya* [Theoretical foundations for identifying sources of information transmitted by blocks of limited size : monograph], Kursk, Publishing House of JSC University Book, 2020. 198 p.

DOI 10.54398/2074-1707_2022_1_93
УДК 681.32; 004.056

СИНТЕЗ СТРУКТУРЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ

Статья поступила в редакцию 29.12.2021, в окончательном варианте – 21.01.2022.

Кочнев Сергей Владимирович, Государственный научно-исследовательский институт приборостроения, 129226, Российская Федерация, г. Москва, пр. Мира, 125,
начальник отдела, ORCID 0000-0001-6226-7518, e-mail: s.v.ko@mail.ru

Лапсарь Алексей Петрович, Управление ФСТЭК России по Южному и Северо-Кавказскому федеральным округам, 344079, Российская Федерация, г. Ростов-на-Дону, ул. Ярослава Галана, 1е/25,
кандидат технических наук, доцент, заместитель начальника отдела, ORCID 0000-0003-2273-725X, e-mail: lapsar1958@mail.ru

Барабошкина Алена Владимировна, Ростовский государственный экономический университет (РИНХ), 344002, Российская Федерация, г. Ростов-на-Дону, ул. Большая Садовая, 69,
магистрант, e-mail: alenaas64@mail.ru.

Отмечается, что безопасная реализация критических производственных процессов в сферах здравоохранения, науки, транспорта, связи, энергетики и других во многом обеспечивается эффективностью функционирования объектов критической информационной инфраструктуры. Указаны проблемы применения информационных технологий в объектах критической информационной инфраструктуры, связанные с повышением их уязвимости к деструктивным воздействиям, реализуемым с помощью удаленного доступа. Установлено, что в настоящее время защита от деструктивных информационных воздействий сводится к прекращению обмена с внешней средой и остановке производственного процесса, что приводит к снижению его эффективности. Проанализированы особенности эксплуатации объектов критической информационной инфраструктуры в условиях деструктивного информационного воздействия и обоснованы требования к ним. Перспективные методы и модели оценки и прогнозирования состояния сложных технических систем распространены на объекты критической информационной инфраструктуры. В качестве информативного параметра в параметризованных моделях объектов информационной инфраструктуры предложено использовать свойства и характеристики деструктивных информационных воздействий. С применением методов структурного синтеза на основе диффузионных марковских моделей разработана обобщенная структура объекта критической информационной инфраструктуры, реализующего диагностические и управляющие функции. Рассмотрен вариант функционирования такого объекта в нормальных и нештатных условиях эксплуатации. Результатами проведенного исследования явилась разработка универсальных требований к объектам критической информационной инфраструктуры, реализующих управление критическими процессами, и обобщенная структура такого объекта. Полученные результаты применимы при разработке перспективных или модернизации существующих объектов критической информационной инфраструктуры критических производственных процессов и реализованы в техническом задании на разработку автоматизированной системы управления субъекта критической информационной инфраструктуры, функционирующего в сфере науки.

Ключевые слова: критический процесс, объект критической информационной инфраструктуры деструктивное информационное воздействие, аварийная ситуация, структура, эволюционные уравнения, параметризованные марковские модели