УДК 681.324

И.В. Рубан[1], С.В. Дуденко[2], А.А. Смирнов[2]

[1] *Харьковский национальный университет радиоэлектроники, Харьков*
[2] *Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков*

ПОДХОД К ОЦЕНИВАНИЮ УЯЗВИМОСТИ СТЕГАНОГРАФИЧЕСКОГО КАНАЛА НА ОСНОВЕ УСЕЧЁННОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ В ПОЛЕ ГАЛУА К АТАКЕ «ПО ИЗВЕСТНОЙ МАТЕМАТИЧЕСКОЙ МОДЕЛИ»

В данной статье приведены результаты анализа уязвимости сетевого стеганографического канала к атаке «по известной математической модели». Проведено сравнение распределений значений ISN при управлении их генерацией операционной и стеганографической системами. Предложено использование усечённого преобразования Фурье в поле Галуа для приобретения равномерного характера распределения начальных номеров последовательностей (ISN), генерируемых стеганографической системой.

Ключевые слова: *сетевая стеганография, усечённое преобразование Фурье в поле Галуа, начальный номер последовательности.*

Введение

Постановка задачи. Опыт последних вооруженных конфликтов показывает, что главным направлением обеспечения информационной безопасности государства является защита его киберпространства [1].

Возрастающие требования к обеспечению кибернетической безопасности определяют постоянно растущее количество угроз и, соответственно, развитие методов защиты данных, обрабатываемых в информационных телекоммуникационных сетях (ИТКС).

Зачастую, с целью обеспечения целостности и доступности информационных ресурсов, приходится жертвовать оперативностью передачи важных данных, что в некоторых случаях приводит к снижению эффективности управления.

Анализ последних исследований и публикаций. В последнее время, приобрели популярность методы скрытной передачи данных в ИТКС, использующие особенности протоколов базовой эталонной модели сетевого взаимодействия (БЭМСВ) [1, 2]. Все протоколы БЭМСВ исполнены в виде стандартов RFC (Request For Comments) и носят рекомендательный характер, не принуждая к реализации протоколов во всех тонкостях, но акцентируя внимание на применяемости любой разработанной версии. Множество таких методов объединяет в себе «сетевая стеганография», основной задачей которой, является сокрытие самого факта передачи сообщения, что усиливает систему защиты информации еще одним уровнем.

Метод стеганографической передачи данных, описанный в [1], основан на возможности перехвата управления генерацией начальных номеров последовательности (Initial Sequence Number – ISN) при установлении соединения по протоколу транспортного уровня TCP [2]. В основе метода лежит поиск соответствий символов скрытно передаваемого сообщения с символами опорного текста, размещаемого в качестве полезной нагрузки протокола TCP.

Эффективность стеганографических методов, в целом, можно оценить по их устойчивости к известным типам атак. Атаки на стеганографические системы (СГС) сводятся к: выявлению функционирования СГС; чтению, удалению и изменению скрытно передаваемых сообщений без внесения существенных изменений в стегоконтейнер.

Важной особенностью метода стеганографической передачи данных, описанного в [1], является то, что малейшее изменение в стегоконтейнере (изменение или удаление сообщения), приводит к нарушению функционирования протокола TCP. Это связано с защитными механизмами протокола, которые обеспечивают надёжность доставки данных. Для чтения сообщений, необходимо сначала выявить TCP-сокет, в пределах которого функционирует СГС, а их количество может достигать нескольких десятков для каждого клиента, обслуживающего его сервера. Для проведения анализа, на предмет наличия характеристических признаков функционирования стеганографического канала (СГК), необходима возможность сбора и обработки необходимых статистических данных.

Применение предлагаемого в [3] метода стеганографической передачи данных в чистом виде, приводит к его уязвимости к атаке “по известной математической модели”.

Целью статьи является модификация метода стеганографической передачи данных в ИТКС на основе генерации ISN tcp-соединений, для достижения его стеганографической стойкости к атаке“по известной математической модели”.

Основная часть

Для оценки уязвимости СГК предлагается подход, состоящий из следующих основных этапов.

1. Определение характера распределения значений ISN, при управлении генерацией ISN операционной системой (ОС).

2. Определение характера распределения значений ISN, при управлении генерацией стеганографической системы.

3. Использование усечённого преобразования Фурье над полем Галуа для получения равномерного характера распределения ISN.

При использовании такого подхода, ожидаемым результатом, является равномерный характер распределения значений ISN, используемых в стеганографическом канале.

Определение характера распределения значений ISN при управлении генерацией ОС

При управлении генерацией начальных номеров последовательности операционной системой (Windows 7 x64 professional), их значения распределены равномерно на произвольно выбранном интервале наблюдения (рис. 1).

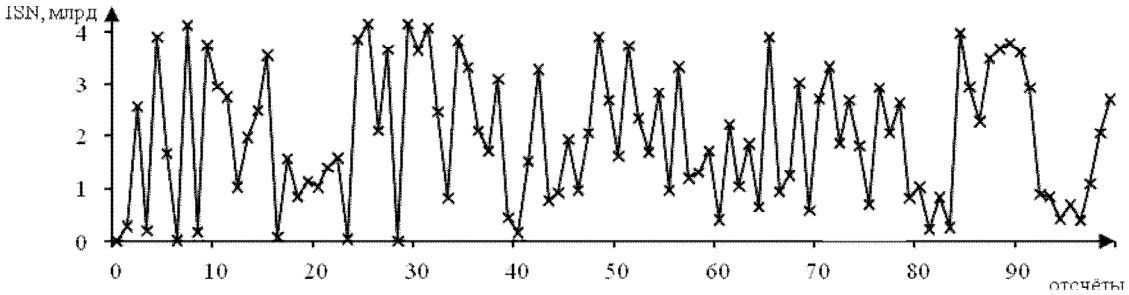

Рис. 1. Распределение значений начальных номеров последовательности при управлении их генерацией операционной системой (Windows 7 x64professional)

Статистика, результаты которой представлены в виде графика на рис. 1, была получена посредством проведения DoS-атаки, типа «SYN-флуд». Сбор статистики производился на «третьем» хосте в результате перевода сетевого адаптера в «беспорядочный режим» (promiscuous mode) и использовании программы–сниффера. Фильтры сниффера были настроены на перехват всех TCP SYN-фрагментов атакующего хоста.

Для проверки гипотезы о законе распределения ISN использован критерий согласия Пирсона «Хи-квадрат» [6].

Выдвигаемые гипотезы о законе распределения величины ISN, при управлении её генерацией операционной системой, следующие.

H0 – основная гипотеза.

Распределение дискретной случайной величины ISN – равномерное.

H1 – альтернативная гипотеза.

Распределение дискретной случайной величины ISN отличное от равномерного.

$$\chi^2_{\text{набл}} = \sum_{i=1}^{8} \frac{(n_i - n_i^*)^2}{n_i^*} = 8{,}67\,; \qquad (1)$$

$$\chi^2_{\text{кр}}(7;0{,}05) = 14{,}06\,; \qquad (2)$$

$$\chi^2_{\text{кр}} > \chi^2_{\text{набл}}\,; \quad 14{,}06 > 7{,}01\,. \qquad (3)$$

Из (3) следует, что наблюдаемое значение статистики Пирсона, меньше критического значения. Это означает, что принимается основная гипотеза.

Определение характера распределения значений ISN при управлении генерацией СГС

При управлении генерацией начальных номеров последовательности стеганографической системой, их распределение имеет вид вид, представдены на рис. 2.

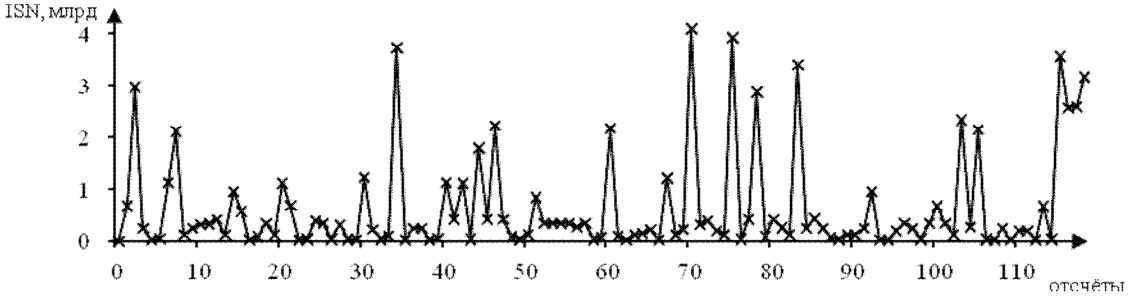

Рис. 2. Распределение значений начальных номеров последовательности при управлении их генерацией стеганографической системой

Выдвигаемые гипотезы о законе распределения дискретной случайной величины ISN при управлении её генерацией стеганографической системы следующие:

H0 – основная гипотеза.

Распределение дискретной случайной величины ISN – равномерное.

H1 – альтернативная гипотеза.

Распределение дискретной случайной величины ISN – отличное от равномерного.

$$\chi^2_{\text{набл}} = \sum_{i=1}^{8} \frac{(n_i - n_i^*)^2}{n_i^*} = 43{,}25; \qquad (4)$$

$$\chi^2_{\text{кр}}(7;0{,}05) = 14{,}06; \qquad (5)$$

$$\chi^2_{\text{кр}} < \chi^2_{\text{набл}}; \quad 14{,}06 < 43{,}66. \qquad (6)$$

Из (6) следует, что наблюдаемое значение статистики Пирсона, меньше критического значения. Это означает, что основная гипотеза отвергается.

Исходя из описанного выше, можно сделать вывод о том, что метод стеганографической передачи данных на основе генерации ISN TCP-соединений неустойчив к атаке «по известной математической модели», так как даёт распределение значений ISN, отличное от равномерного.

Использование усечённого преобразования Фурье над полем Галуа для достижения равномерного характера распределения ISN

При поиске подходящего преобразования, был исследован ряд линейных преобразований, возможных в конечном поле. Это связано с тем, что исходной, при вычислении ISNвеличиной, является вектор, состоящий из четырёх элементов (рис. 3, $v = \{87,77,93,67\}$).

Линейные преобразования в конечном поле, обладают рядом недостатков, поэтому было выбрано усечённое преобразование Фурье (УПФ) над полем Галуа [7]. Данное преобразование является нелинейным и двусторонним (7), (8), что позволяет восстанавливать исходные значения на стороне получателя.

Результаты исследований, при поиске подходящего преобразования из числа линейных, в статье не отображены, так как являются отрицательными.

В [7] доказана теорема о существовании усеченного унитарного преобразования Фурье в конечном поле.

$$V_j = \sum_{i=1}^{n-1} w^{ij} \cdot v_i; \qquad (7)$$

$$v_i = \left(\frac{1}{n \bmod p}\right) \sum_{j=1}^{n-1} \left(w^{-ij} \oplus L\right) \cdot V_j, \qquad (8)$$

где w – элемент порядка n в поле $GF(q)$;

$\oplus$ – означает операцию сложения в поле;

L=-1.

Нелинейность преобразования достигается за счёт изменения порядка выполнения операций в поле при вычислении значений выходного вектора [4].

В данном случае, входным для УПФ вектором, будет являться четырёхбайтный блок 32-разряднго ISN (рис. 3).

На рис. 3 для

$$ISN = 41269827_{10} = 00010100010101110101110101000011_2,$$

проиллюстрировано получения входного вектора и выполнение прямого усечённого преобразования Фурье.

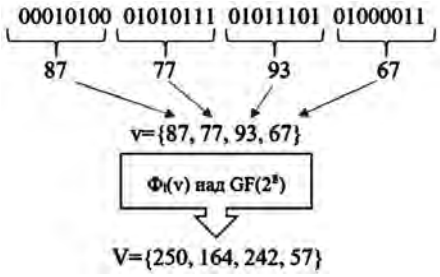

Рис. 3. Получение входного вектора v и выполнение УПФ над полем $GF(2^8)$

В результате выполнения преобразования (7) над множеством номеров ISN, полученных при управлении их генерацией СГС, получено распределение, представленное на рис. 4.

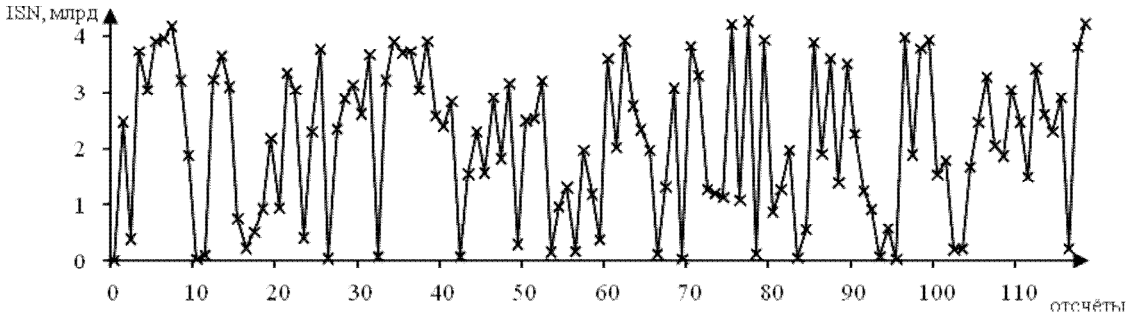

Рис. 4. Распределение ISN*, полученное в результате применения УПФ над блоками значений, вычисляемыми СГС при формировании ISN

Для проверки гипотезы о законе распределения дискретной случайной величины ISN* использован критерий согласия Пирсона «Хи-квадрат» [3].

Выдвигаемые гипотезы о законе распределения дискретной случайной величины ISN* при управлении её генерацией операционной системой следующие.

H0 – основная гипотеза. Распределение дискретной случайной величины ISN* – равномерное.

H1 – альтернативная гипотеза. Распределение дискретной случайной величины ISN* отличное от равномерного.

$$\chi^2_{\text{набл}} = \sum_{i=1}^{8} \frac{(n_i - n_i^*)^2}{n_i^*} = 11{,}33\,; \qquad (9)$$

$$\chi^2_{\text{кр}}(7;0{,}05) = 14{,}07\,; \qquad (10)$$

$$\chi^2_{\text{кр}} > \chi^2_{\text{набл}}\,; \quad 14{,}07 > 11{,}33\,. \qquad (11)$$

Из (3) следует, что наблюдаемое значение статистики Пирсона, меньше критического значения. Это означает, что принимается основная гипотеза.

Выводы

В результате усечённого преобразования Фурье в поле Галуа над блоками значений, вычисляемыми при формировании начальных номеров последовательности TCP, характер распределения является равномерным. Полученный результат позволяет утверждать, что за счёт использования УПФ, предложенный метод стеганографической передачи данных становится устойчивым к атаке «по известной математической модели», а характер распределения значений начальных номеров последовательности, при управлении их генерацией операционной системой, будет неотличим от характера распределения ISN*.

Список литературы

1. Рубан И.В. Anapproachtocybersecuritysupport / И.В. Рубан // Системи обробки інформації. – 2015. – № 11(136). – С. 6-8.

2. Орлов В. П. Методы скрытой передачи информации в телекоммуникационных сетях: дис. ... кандидата технических наук: 05.12.13 / Орлов Владимир Владимирович. – Самара, 2012. – 166 с.

3. Рубан И.В. Метод стеганографической передачи данных в информационно-телекоммуникационных сетях на основе генерации ISN tcp-соединений / И.В. Рубан, А.О. Смирнов // Системи обробки інформації. – Х.: ХУПС, 2015. – № 9 (134). – С. 99-101.

4. "Instructions to RFC Authors" RFC-2223. Category: Informational / Network Working Group, October 1997 [Electr. resource]. – Accessed to: https:// http://rfc2.ru/2223.rfc/original.

5. "Internet protocol - DARPA Internet Program Protocol Specification" RFC-793. TCP. USC / Information Sciences Institute, September 1981 [Electr. resource]. – Accessed to: https://www.rfc-editor.org/rfc/rfc793.txt.

6. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высш. шк., 1977. – 479 с.

7. Долгов В.И., Рубан И.В., Дуденко С.В. Построение нелинейных систем на основе усеченного преобразования Фурье в конечных полях / В.И. Долгов, И.В. Рубан, С.В. Дуденко // Радиотехника: сб. научн. тр. – Х.: ХНУРЭ, 2003. – Вып. 134. – С. 121-131.

Поступила в редколлегию 14.12.2015

Рецензент: д-р техн. наук, проф. К.С. Смеляков, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ПІДХІД ДО ОЦІНЮВАННЯ ВРАЗЛИВОСТІ СТЕГАНОГРАФІЧНОГО КАНАЛА НА ОСНОВІ УСІЧЕНОГО ПЕРЕТВОРЕННЯ ФУР'Є В ПОЛІ ГАЛУА ДО АТАКИ «ЗА ВІДОМОЮ МАТЕМАТИЧНОЮ МОДЕЛЛЮ»

І.В. Рубан, С.В. Дуденко, А.О. Смірнов

У даній статті наведено результати аналізу уразливості мережевого стеганографічного каналу до атаки «за відомою математичної моделлю». Проведено порівняння розподілів значень ISN при управлінні їх генерацією операційної та стеганографічної системами. Запропоновано використання усіченого перетворення Фур'є в полі Галуа для придбання рівномірного характеру розподілу початкових номерів послідовності (ISN), що генеруються стеганографічної системою.

Ключові слова: *мережева стеганографія, усічене перетворення Фур'є в полі Галуа, початковий номер послідовності.*

THE APPROACH TO THE ASSESSMENT OF VULNERABILITY STEGANOGRAPHIC CHANNEL BASED ON THE TRUNCATED FOURIER TRANSFORM IN GALOIS FIELD TO ATTACK "BY A KNOWN MATHEMATICAL MODELS"

I.V. Ruban, S.V. Dudenko, A.A. Smirnov

The results of the analysis of the vulnerability of the network to the steganographic channel attack "by a known mathematical model" has been presents in this article.TheDistributions of ISN values in the management of their generation operating systems and steganography has beenanalyzed. Using of the truncated Fourier transform in Galois field for the purchase of a uniform nature of the distribution of the initial sequence number (ISN) which generate by steganographic system has been proposed.

Keywords: *network steganography, truncated Fourier transform in Galois field, initial sequence number.*