В данной работе проводится определение показателей выходных последовательностей шифров гаммирования на основе динамического хаоса с использованием метода сингулярного спектрального анализа. Определяется уровень главных компонент, меры отклонения от равномерного распределения. Визуализация информации производится в виде фазовых диаграмм, в которых по осям координат откладываются различные пары собственных векторов или главных компонент.

Вычислительный эксперимент проводился при использовании шифра гаммирования на основе динамического хаоса. Схема алгоритма – сеть Фейстеля, отображение пилообразное, число итераций z изменялось от одной до 1024. Длина анализируемых последовательностей $N = 10000$, длина гусеницы $M = 1000$. Результаты расчета уровня главных компонент I для открытого текста (1), шифра гаммирования на основе динамического хаоса при числах итераций $z = 8$ (2), $z = 64$ (3), а также шифров des в режиме cbc (4) и aes в режиме cbc (5) приведены в таблице

Табл. 1. Уровень главных компонент I, открытого текста (откр. текст), выходных последовательностей шифра гаммирования на основе динамического хаоса при числе итераций $z = 8$, $z = 64$, *шифра des в режиме cbc(des_cbc)*

Ном.гл.комп.	1000	999	998	997	996	995	994	993
1	0,3530	0,3530	0,3036	0,3035	0,2989	0,2979	0,2934	0,2934
2	0,2203	0,2202	0,2122	0,2118	0,2081	0,2080	0,2028	0,2027
3	0,226	0,2258	0,2250	0,2250	0,2109	0,2108	0,2015	0,2014
4	0,1899	0,1893	0,1880	0,1879	0,1841	0,1840	0,1821	0,1820
5	0,2287	0,2287	0,2179	0,2177	0,2135	0,2134	0,2083	0,2081

Как видно из таблицы 1, для открытого текста уровень главных компонент I (1) превышает значения для показателей исследуемых шифров (2-5), в среднем, на 50-60 процентов. Сравнительный анализ показателей, полученных для выходных последовательностей шифра гаммирования на основе динамического хаоса, практически совпадает с показателями, реализуемых шифрами des в режиме cbc и aes в режиме cbc.

ПЕРЕПОЛНЕНИЕ БУФЕРА: ПРОШЛОЕ, НАСТОЯЩЕЕ И БУДУЩЕЕ

Фомчин Д. О.

БГУ, НИИ ППМИ, Минск, Беларусь, e-mail: dimafomchin@gmail.com

Переполнение буфера по праву считается одной из самых опасных уязвимостей. При эксплуатировании появляется практически неограниченный доступ к атакуемой системе. Переполнение буфера известно ещё с самого появления компьютеров, и вот теперь, сквозь десятилетия, эта проблема не решена полностью.

Всего в базе бюллетеней по безопасности Microsoft около 1000 записей. Большинство из отмеченных уязвимостей относятся к переполнению буфера. Самые опасные – это те, которые позволяют удалённо выполнить произвольный код без участия пользователя, т.е. не требуется открывать файлы или заходить на какой-либо интернет-ресурс. Вот одни из этих уязвимостей:

MS00-066, MS00-091, MS01-048, MS03-010, MS03-026, MS03-033, MS03-039, MS04-011, MS04-012, MS04-029, MS04-036, MS05-019, MS05-034, MS06-032, MS06-040, MS07-029, MS07-035, MS08-001, MS08-059, MS08-067, MS08-068, MS09-001, MS09-048, MS09-049, MS09-053, MS09-064, MS09-071, MS10-009, MS10-012, MS10-040, MS10-054, MS10-061, MS10-065, MS10-066, MS11-019, MS11-020, MS11-030, MS11-042, MS11-053, MS11-058, MS11-083, MS11-095, MS12-020.

Здесь собраны те, которые могут быть эксплуатированы удалённо, без участия пользователя и без установки посторонних приложений. Всё, что нужно - это компьютер с уязвимой версией операционной системы, подключённый к сети.

Переполнение буфера используется и для запуска «червей» на компьютер. Самый известный пример – Blaster Worm (MSBlast). Для распространения использовались уязвимости MS03-026 и MS03-039.

Было предпринято много попыток борьбы с этой уязвимостью с помощью как программных, так и аппаратных решений. Различные средства контроля встраиваются в операционные системы всех производителей для персональных компьютеров, мобильных устройств, серверов.

Недавно обнаруженная критическая уязвимость MS12-020 в операционных системах Windows получила широкое обсуждение в интернете. Подверженными к атаке оказались все операционные системы Microsoft Windows, начиная с Windows XP и заканчивая Windows 7 и Windows Server 2008. Несмотря на всё это сегодня доступен только один эксплоит, позволяющий вызвать отказ в обслуживании. Эксплоит, позволяющий выполнить произвольный код, не разработан до сегодняшнего дня. Если всё же появится эксплоит, будет ли он работать в современных операционных системах Windows 7, Windows 8 и Windows Server 2008? Дают ли современные методы защиты доступные в этих операционных системах гарантию безопасности? Эти вопросы мы и обсудим.

Литература

1. Michael Howard, David LeBlanc. Writing Secure Code Second Edition. Microsoft Press, 2004.
2. Бюллетень по безопасности (Майкрософт) MS12-020 [Электронный ресурс]. Режим доступа: http://technet.microsoft.com/ru-ru/security/bulletin/ms12-020. -Дата доступа: 11.04.2012.