барьеров вокруг CNL. Заявляемая модель сети — композитная стволовая — предполагает связи между узлами как бинарные отношения трех типов: связь-«крепление» (B-связь), описывающая взаимодействие узлов одного и того же ствола; связь-«соединение» (C-связь), для узлов заданного слоя обособленной стволовой сети (отдельной клумбы) подобно связи в традиционной «плоской» комплексной сети; наконец, связь-«зависимость» (D-связь), управляющая взаимодействием между узлами различных стволов (принадлежащих различным клумбам) одного и того же букета. Такая детализация связей способствует глубокому пониманию реальных сетевых процессов и объективной постановке задач при моделировании атак на отдельные элементы сети (узлы, стволы, букеты, клумбы, слои, B-, C- и D-связи) и их комбинации. В рамках данной модели элементы сети реальной критической инфраструктуры рассматриваются как стволы, которые являются автономными или взаимосвязанными и взаимозависимыми как внутри, так и за пределами государства, региона и местной территории. Так, большинство объектов критической инфраструктуры, являющихся собственностью федеральных, региональных или местных органов власти или частного сектора, могут быть стратифицированы по различным слоям и соответствующим клумбам, одновременно оставаясь связанными с другими системами той же или иной природы. Композитное стволовое представление сети также дает возможность учесть многие топологические уязвимости реальных систем, что позволило дополнить классификационную схему атак [5].

Выводы. Предложена модель, формализующая сложные взаимодействия элементов сетей различной природы. Предполагается особо успешным и значимым применение данной модели к задачам управления чрезвычайными ситуациями. Сопутствующая классификация атакующих действий может быть полезна при анализе уязвимости не только абстрактных сетевых моделей, но и реальных систем.

СПИСОК ЛИТЕРАТУРЫ:

1. *Barabási A.-L., Albert R., Jeong H.* Mean-field theory for scale-free random networks // Physica A. 1999. Vol. 272. P. 173–187.
2. *Gao J., Buldyrev S. V., Stanley H. E., Havlin S.* Networks formed from interdependent networks // Nature Physics. 2012. Vol. 8. P. 40–48. URL: http://www.nature.com/nphys/journal/v8/n1/pdf/nphys2180.pdf (дата обращения: 21.12.2012).
3. *Тихомиров А. А., Труфанов А. И., Носырева Л. Л., Носырева Е. В.* Математическое описание стволовых сетей // Труды XVII Байкальской Всероссийской конференции. Т. 3. Иркутск, 2012. С. 149–153.
4. *Cheng H. K., Guo H.* Computer Virus Propagation in a Network Organization: The Interplay between Social and Technological Networks. Working Paper № 08-24, October 2008. – 28 p. URL: http://archive.nyu.edu/bitstream/2451/29495/2/Cheng_Guo_08-24.pdf (дата обращения: 21.12.2012).
5. *Тихомиров А. А., Труфанов А. И., Дмитриенко В. Н., Россодивита А., Шубников Е. В.* Классификация атак в имитационных исследованиях уязвимости комплексных сетей // Безопасность информационных технологий. 2012. № 1. С. 46–52.

Г. И. Хоруженко, М. А. Пудовкин

О СВОЙСТВАХ ЛИНЕЙНОГО АЛГОРИТМА РАЗВЕРТЫВАНИЯ КЛЮЧА БЛОЧНОЙ ШИФРСИСТЕМЫ SMALLPRESENT

Обобщенная блочная шифрсистема SmallPresent была представлена в работе [1] с целью детального исследования атак на блочную шифрсистему PRESENT. Так, например, в работах

[2–3] предполагается использование всего множества пар открытых текстов и шифртекстов для успешного проведения атаки, что делает невозможным их проверку на практике. В настоящей работе рассматривается стойкость данной обобщенной шифрсистемы с произвольным линейным алгоритмом развертывания ключа к анализу линейным методом с целью определения параметров алгоритма развертывания ключа, обеспечивающих необходимый уровень стойкости, а также экспериментального подтверждения полученных теоретических оценок.

Обозначим V_n — пространство двоичных векторов размерности n, $S(X)$ — симметрическая группа, заданная на множестве X, «$\cdot$» — операция побитового умножения векторов.

Приведем описание обобщенной шифрсистемы SmallPresent. Пусть заданы $n = tm, m \in \mathbb{N}$ — длина блока открытого текста, $t \in \mathbb{N}$ — размер s-бокса. Пусть также заданы преобразования $\hat{s} = (\underbrace{s, \ldots, s}_{m}), s \in S(V_t)$, $h : V_n \to V_n$, $h((\alpha_{n-1}, \ldots, \alpha_0)) = (\alpha_{\sigma(n-1)}, \ldots, \alpha_{\sigma(0)})$, $\sigma \in S_{n-1}$. Таким образом, раундовая функция для j-го раунда имеет вид

$$g_k^{(j)}(\alpha) = \hat{s}\left(h\left(\alpha \oplus k^{(j)}\right)\right),$$

где $k^{(j)} \in V_n$ — раундовый ключ j-го раунда. В работе предполагается, что $k^{(j)} = \boldsymbol{a}^j k \oplus c^{(j)}$, где $\boldsymbol{a}$ — $n \times n$ матрица над $GF(2)$, $k \in V_n$ — ключ шифрования, $c^{(j)}$ — константа, зависящая от номера раунда j.

Для оценки стойкости шифрсистемы используется следующий подход.

Алгоритм 1 строит линейные характеристики, вероятность которых не меньше $2^{-\frac{n}{2}}$, а также вычисляет максимальное число раундов для найденных характеристик. Каждая характеристика $\varphi = \gamma_1 \cdot \alpha^{(0)} \oplus \gamma_2 \cdot \alpha^{(r_0)} \oplus \gamma_3 \cdot k$, где $\gamma_1, \gamma_2, \gamma_3 \in V_n$, представляет собой линейную комбинацию битов блоков открытого текста и шифртекста и ключа шифрования.

Алгоритм 2 на основе поданных на вход линейных характеристик находит матрицу $\boldsymbol{a}$, такую, что выполнено условие:

$$\left| n - \|\gamma_3\| \right| < \frac{\delta n}{2},$$

где $\delta \in (0,1]$ — наперед заданный параметр, характеризующий стойкость к анализу линейным методом.

Последовательно применяя алгоритмы 1 и 2, получаем искомый алгоритм развертывания ключа для заданной блочной шифрсистемы.

Описанный метод применен для анализа шифрсистемы SmallPresent с s-боксом

$s_0 = (4,10,9,2,13,8,0,14,6,11,1,12,7,15,5,3)$

из тестового набора алгоритма ГОСТ 28147-89 и длинами блоков открытого текста $n \in \{12, \ldots, 64\}$. В результате эксперимента получен класс алгоритмов развертывания ключа, обеспечивающих стойкость блочной шифрсистемы SmallPresent относительно линейного метода анализа. Полученные значения параметров линейных характеристик и матриц приведены в таблице 1.

Таблица 1. Результаты работы алгоритмов 1 и 2 для s-бокса s_0.

Длина блока n	Минимальное число раундов r_0	Вероятность линейной характеристики	Длина ключа	Число битов ключа в линейной комбинации
12	6	2^{-6}	12	12
16	6	2^{-7}	16	15
20	7	2^{-9}	20	19
24	7	2^{-10}	24	22

28	7	2^{-13}	28	27
32	8	2^{-16}	32	30
36	9	2^{-17}	36	35
40	9	2^{-19}	40	39
44	9	2^{-22}	44	41
48	10	2^{-23}	48	47
52	10	2^{-24}	52	50
56	11	2^{-26}	56	55
60	11	2^{-30}	60	58
64	11	2^{-31}	64	61

Из таблицы видно, что длина ключа, необходимая для того, чтобы шифрсистема была стойкой к линейному методу анализа на заданном числе раундов, равна длине блока открытого текста для всех проведенных экспериментов.

Гипотеза. Пусть $\delta \in (0,1]$. Для любого $n \in \mathbb{N}$ существует алгоритм развертывания ключа блочной шифрсистемы SmallPresent, обеспечивающий ее стойкость к анализу линейным методом при использовании ключа шифрования длины n.

СПИСОК ЛИТЕРАТУРЫ:

1. *Leander G.* Small scale variants of the block cipher PRESENT. Cryptology ePrint Archive, Report 2010/143.
2. *Nakahara J., et al.* Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT // Proceedings of CANS'09. Vol. 5888. P. 58–75.
3. *Ozen O., Varici K.* Lightweight block ciphers revisited: Cryptanalysis reduced round PRESENT and HIGHT // Lecture Notes in Computer Science. 2009. Vol. 5594. P. 90–107.

Э. Э. Яндыбаева, И. В. Машкина

ПОЛИТИКА БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ НА ПРЕДПРИЯТИИ

В основе информационной безопасности (ИБ) предприятия лежит комплект документов, включающих в себя концепцию ИБ, модель угроз и нарушителя, политику ИБ, технологические инструкции для сотрудников и т. д. Для обеспечения безопасного использования электронной подписи (ЭП) необходимо создание частной политики безопасности использования ЭП. На рис. 1 показана иерархия документов по ИБ. Ниже приводится текст разработанной политики безопасности использования ЭП.