представлены графически атаки согласно уровню их воздействия в условиях модели OSI. Атаки на физическом уровне используют физические особенности каналов передачи информации. Атаки на канальном уровне используют информацию из заголовка канального уровня. Атаки на сетевом уровне используют протоколы сетевого уровня (IP, ICMP, ARP, протоколы маршрутизации). Атаки, использующие протоколы транспортного уровня, такие как TCP, UDP. Самая интересная для рассмотрения в условиях концептуальной модели OSE/RM группа атак — это атаки прикладного уровня, к ним относятся: внедрение вирусов и троянских программ, использование уязвимостей ОС и прикладного ПО, подбор паролей, атаки на веб-приложения типа CSS (Cross-Site Scripting) и SQL Injection и т. д. Графическое представление атак в рамках модели OSE/RM позволяет создать новый подход к построению моделей безопасности открытых систем. Мы ставим своей целью в последующих публикациях отобразить в рамках модели OSE/RM классические модели управления доступом, проработка по данным направлениям ведется и ее результаты отображены в [2, 4]. Например, реализация субъектно-ориентированной модели изолированной программной среды позволяет определить порядок безопасного взаимодействия субъектов системы, что дает защиту от внедрения вредоносного ПО.

СПИСОК ЛИТЕРАТУРЫ:

1. IEEE Std 1003.0-1005, IEEE Guide to the POSIX Open System Environment (OSE). N-Y.: The Institute of Electrical and Electronics Engineers, 1995. — 194 p.
2. *Лукинова О. В.* Структуризация функций защиты в соответствии с моделью OSE/RM // Тезисы XIX Всероссийской школы-коллоквиума по стохастическим методам и XIII Всероссийского симпозиума по прикладной и промышленной математике (Сочи — Вардане, 1–8 октября 2012 г.). URL: http://www.tvp.ru/conferen/vsppm13/petso206.pdf (дата обращения 20.01.2013).
3. *Бойченко А. В., Кондратьев В. К., Филинов Е. Н.* Основы открытых информационных систем. 2-е издание, переработанное и дополненное. Под ред. В. К. Кондратьева. М.: Издательский центр АНО «ЕОАИ», 2004. — 128 с.
4. *Бойченко А. В., Лукинова О. В.* Применение модели POSIX OSE/RM при построении подсистем информационной безопасности // Труды Международной конференции «Интеллектуальные системы» (AIS10). Т. 2. М.: Физматлит, 2010. С. 473–476.

М. А. Куприяшин, Г. И. Борзунов

АНАЛИЗ СОСТОЯНИЯ РАБОТ, НАПРАВЛЕННЫХ НА ПОВЫШЕНИЕ СТОЙКОСТИ ШИФРСИСТЕМ НА ОСНОВЕ ЗАДАЧИ О РЮКЗАКЕ

Системы на основе задачи о рюкзаке изначально оказались нестойкими [1, 2, 3]; были созданы эффективные методы анализа, позволяющие достаточно быстро взломать эти шифрсистемы (в частности, шифрсистемы Меркля — Хэллмана [4], Грэхма — Шамира [5]).

Однако в недавних публикациях [6, 7, 8], рюкзачные системы получили дальнейшее развитие, что привело к созданию более стойких шифрсистем. (например, шифрсистема Су [9]). Разработаны и теоретически обоснованы математические модели односторонних функций, основанных на современных модификациях задачи о рюкзаке. Эти модели позволили теоретически обосновать высокую стойкость указанных выше шифрсистем.

Для экспериментальной проверки практической стойкости новых шифров на основе задачи о рюкзаке требуется разработка методики проверки их стойкости при помощи современных средств вычислительной техники

Такая методика позволит не только упростить анализ шифров на основе задачи о рюкзаке впоследствии, но и выявить недостаточную стойкость к анализу у существующих систем.

СПИСОК ЛИТЕРАТУРЫ:

1. *Adleman L.* On Breaking Generalized Knapsack Public Key Cryptosystems // Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing. M., 1983. С. 402—412.
2. *Shamir A.* A Polynomial-time Algorithm for Breaking the Basic Merkle — Hellman Cryptosystem // Proceedings of the IEEE Symposium on Foundations of Computer Science. M., 1982. С. 145—152.
3. *Lai M. K.* Knapsack Cryptosystems: The Past and the Future. 2001.
4. *Merkle R., Hellman M.* Hiding Information and Signatures in Trapdoor Knapsacks // IEEE Transactions on Information Theory. Vol. IT-24. M., 1978. С. 525—530.
5. *Shamir A., Zippel R.* On the Security of the Merkle — Hellman Cryptographic Scheme // IEEE Transactions on Information Theory, vol. IT-26. M., 1998. С. 339—340.
6. *Kasahara M.* Construction of New Classes of Knapsack Type Public Key Cryptosystem Using Uniform Secret Sequence. M., 2012. — 8 с.
7. *Noro K., Kobayashi K.* Knapsack Cryptosystem on Elliptic Curves. M., 2009. — 6 с.
8. *Осипян В.* Разработка математических моделей систем передачи и защиты информации. М., 2006. — 371 с.
9. *Su P. C., Lu E. H., Henry K. C.* A Knapsack Public-key Cryptosystem Based on Elliptic Curves Discrete Logarithm // Applied Mathematics and Computation 168. M., 2005. С. 40—46

С. К. Марфенко, В. О. Чуканов

ПРИМЕНЕНИЕ МОДИФИЦИРОВАННОЙ ЭВРИСТИЧЕСКОЙ МОДЕЛИ НАДЕЖНОСТИ ДЛЯ ОЦЕНКИ УСТОЙЧИВОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В программно-аппаратных системах, которые обеспечивают постоянную возможность для работы клиентов, любой простой или сбой в работе может привести к критическим последствиям. В брокерских приложениях, системах автоматизации бизнес-процессов, где критически важным показателем является коэффициент готовности (вероятность нахождения системы в работоспособном состоянии в произвольный момент времени), каждый отказ ПО приводит к материальным потерям, потерям в качестве и другим потерям для той организации, которая предоставляет такую услугу [1]. По этой причине атака с целью нарушить целостность системы и лишить ее работоспособности может оказаться достаточно серьезной угрозой. Необходимо внимательно подходить к задаче предотвращения такого рода негативных воздействий на систему. Очевидно, что с повышением качества ПО и его надежности уменьшится количество отказов, как случайных, так и запланированных, которые вызываются злоумышленником. Для оценки устойчивости системы к таким атакам целесообразно применять аппарат моделей надежности программного обеспечения, который позволяет сделать оценки некоторых количественных характеристик ПО: количества ошибок, наработки на отказ, вероятности безотказной работы, коэффициента готовности.

В рамках данного доклада рассматривается модифицированная эвристическая модель надежности ПО как аппарат для определения показателей устойчивости. В основе этой модели лежит классическая интуитивная схема: рассматриваемый программный комплекс тестируется