3. ЖТЯИ. 00050-02 30 01 Средство криптографической защиты информации «КриптоПро CSP». Формуляр.
4. ЖТЯИ. 00051-01 30 01 Средство хранения конфиденциальной информации «КриптоПро EFS». Формуляр.
5. *Коротин А. М., Смирнов П. В.* О способах реализации прозрачного шифрования файлов на базе сертифицированного СКЗИ для операционной системы Linux // Безопасность информационных технологий. 2012. № 2.

В. С. Кузнецов

ПРЕДСТАВЛЕНИЕ ИНФОРМАЦИОННЫХ АТАК В УСЛОВИЯХ ЭТАЛОННОЙ МОДЕЛИ OSE/RM

Целью доклада является структурирование угроз открытых информационных систем в соответствии с эталонной моделью POSIX OSE/RM. Согласно определению IEEE POSIX 1003.0 [1], открытой информационной системой называется система, которая реализует открытые спецификации на интерфейсы, сервисы (услуги среды) и поддерживаемые форматы данных, достаточные для того, чтобы дать возможность должным образом разработанному прикладному программному обеспечению быть переносимым в широком диапазоне систем с минимальными изменениями, взаимодействовать с другими приложениями на локальных и удаленных системах и взаимодействовать с пользователями в стиле, который облегчает переход пользователей от системы к системе.

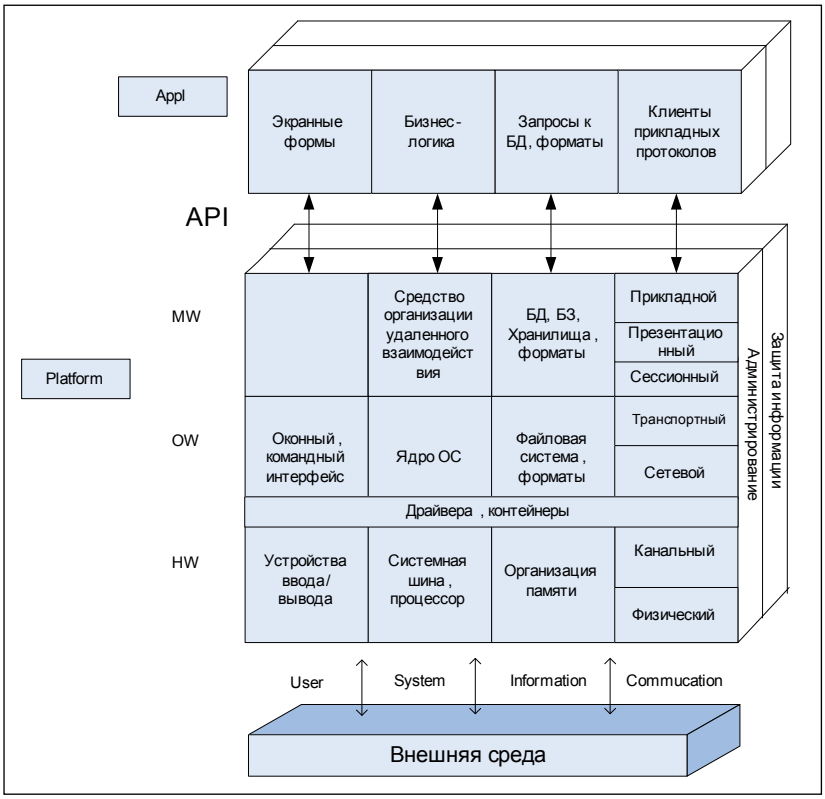

Рис. 1. Концептуальная модель OSE/RM

Если оказалось возможным структурировать информационные системы, то можно структурировать такое понятие, как угрозы безопасности данных систем. Стандарт [1] не потерял своей актуальности и продолжает активно развиваться [2, 3, 4]. В докладе классифицированы и

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