СПИСОК ЛИТЕРАТУРЫ:

1. *Аствацатурьян Е. Р., Беляев В. А., Скоробогатов П. К.* Использование метода КФП для теоретического моделирования и экспериментального исследования радиационного поведения АПОИ на базе ИМС высокой степени интеграции // Специальная техника средств связи. 1987. Вып. 11. С. 3–12.
2. *Барбашов В. М., Трушкин Н. С.* Прогнозирование безопасности микропрограммных БИС в условиях возникновения информационных сбоев // Безопасность информационных технологий. 2008. Вып. 2. С. 61–64.

Е. А. Беляева

АНАЛИЗ ТЕХНИЧЕСКИХ ВОЗМОЖНОСТЕЙ МНОГОФУНКЦИОНАЛЬНЫХ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Цель настоящей работы заключается в анализе технических возможностей современных аппаратно-программных модулей доверенной загрузки (АПМДЗ) и подтверждении необходимости реализации дополнительных функциональных возможностей АПМДЗ в свете их влияния на функциональную безопасность автоматизированных систем в защищенном исполнении (АС ЗИ) [1].

В ходе работы был выполнен анализ технических возможностей современных АПМДЗ, являющихся специальным классом многофункциональных аппаратно-программных средств защиты информации. Рассмотрены основные технические и функциональные возможности модулей, такие как: контроль целостности областей системного реестра, возможность подключения датчиков, наличие дискреционных управляющих выходов и др. Дано их сравнение по рассмотренным возможностям, в частности по управлению в режиме реального времени функционированием средства вычислительной техники с установленным аппаратно-программным модулем доверенной загрузки.

В результате работы были выделены основные дополнительные функции АПМДЗ:

– исключение возможности случайного или намеренного повреждения/вывода из строя платы АПМДЗ электрическими воздействиями (статическое электричество, электрошок) путем реализации электростатической защиты интерфейса считывателя;

– возможность контроля в режиме реального времени физической целостности и режима функционирования средства вычислительной техники, в котором установлен АПМДЗ, за счет реализации интерфейса подключения датчиков;

– возможность управления в режиме реального времени функционированием средства вычислительной техники с установленным АПМДЗ за счет реализации дискретных управляющих выходов;

– исключение возможности случайного или намеренного повреждения/вывода из строя платы АПМДЗ в случае возникновения перепадов или сбоев электропитания средства вычислительной техники с установленным АПМДЗ путем реализации контроля и восстановления целостности служебных структур данных платы АПМДЗ, а также реализации расширенных функций контроля питающих напряжений платы АПМДЗ;

– оснащение платы АПМДЗ сменной флэш-картой типа micro-SD;

– возможность диагностики неисправности по кодам ошибки с использованием индикатора диагностики силами эксплуатирующего персонала.

Таким образом, расширение функциональных возможностей АМПДЗ и создание на их основе многофункциональных аппаратно-программных средств защиты информации обуславливают необходимость проведения дополнительных исследований подобных устройств на предмет оценивания корректности и надежности реализации дополнительных функциональных возможностей АМПДЗ в свете влияния их на функциональную безопасность АС ЗИ в целом [2].

В целях решения поставленной задачи разрабатываются частные методики тестирования различных функциональных подсистем многофункциональных аппаратно-программных средств защиты информации, обеспечивающие оценивание уровня функциональной безопасности всего устройства, в зависимости от архитектуры построения функциональных подсистем и параметров их настроек, а также технических характеристик данных устройств.

СПИСОК ЛИТЕРАТУРЫ:

1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
2. *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. 2-е изд., перераб. и доп. М.: Радио и связь, 2001.

Е. И. Гончаров

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТЫ

С момента своего появления электронная почта была и остается важнейшим инструментом для организации информационного обмена как внутри организации, так и с ее внешними контрагентами. В то же время сам протокол, лежащий в основе ее работы, был создан без учета возможных угроз информационной безопасности. Но не только изначальные просчеты при проектировании протокола снижают уровень его безопасности — электронная почта также является удобнейшим средством Интернета для организации намеренной утечки защищаемой информации.

Основным протоколом электронной почты уже долгое время является ESMTP (Extended Simple Mail Transfer Protocol) [1]. Данный протокол, как и большинство подобных протоколов Интернета, является клиент-серверным и используется для отправки почты от отправителя до сервера и между серверами для дальнейшей пересылки к почтовому серверу получателя.

Сообщение электронной почты представляет собой текстовое сообщение, состоящее из двух обязательных частей: служебного заголовка и тела сообщения, разделенных пустой строкой. Сообщение может содержать только 7-битные символы, т. е. символы таблицы ASCII. При необходимости передать 8-битные данные, например русский текст или бинарные данные, производится их кодирование в печатные символы таблицы ASCII по схеме Base64. Никакого механизма защиты — шифрования сообщения, проверки подлинности отправителя — протокол не предусматривает.

На всех этапах передачи сообщения, кроме последнего — получения письма адресатом — используется один и тот же протокол (E)SMTP. На последнем шаге могут использоваться различные протоколы — POP3, IMAP. Процесс передачи сообщения выглядит следующим образом: