ИССЛЕДОВАНИЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «МАГПРО КРИПТОПАКЕТ»

В.С. Сляднев, Д.Е. Белов, Е.А. Сляднева

Средство криптографической защиты информации (СКЗИ) «МагПро КриптоПакет» основана на программных продуктах с открытым исходным кодом

OpenSSL и OpenVPN. Разработчикам удалось заменить алгоритмы шифрования с RSA на ГОСТ, в соответствии с руководящими документами ФСБ в Российской Федерации. «OpenVPN-ГОСТ» предлагает масштабируемый режим клиент/сервер, позволяет нескольким клиентам подключаться к одному и тому же серверному процессу «OpenVPN-ГОСТ» через один TCP-порт. «OpenVPN-ГОСТ» – это составная часть СКЗИ «МагПро КриптоПакет» 3.0, а именно исполнение 7 (соответствует классу КС1) и исполнение 8 (соответствует классу КС2) указанного СКЗИ. При выявлении нарушений целостности модулей СКЗИ или операционной системы необходимо выявить и устранить причины искажения модулей. Восстановление целостности СКЗИ осуществляется с помощью средств установки СКЗИ или программного комплекса, использующего СКЗИ: для Windows путем повторной установки СКЗИ; для UNIX-подобных ОС – путем повторной установки пакета в режиме «reinstall». Перед установкой СКЗИ необходимо проверить целостность дистрибутивных пакетов СКЗИ (перечень дистрибутивных пакетов и значения хэш-векторов для них приведены в формуляре на СКЗИ). По завершении процедур восстановления целостности модулей СКЗИ и/или операционной системы должна быть проведена проверка корректности восстановления путем вычисления хэшвекторов модулей и их сравнения с ранее зафиксированными эталонными значениями [1–10].

Литература

1. Ярочкин В.И. Информационная безопасность. М.: Международные отношения, 2014. 640 с.
2. Степанов Е.А. Информационная безопасность и защита информации. М.: ИНФР-М, 2014. 353 с.
3. Северин В.А. Правовое обеспечение информационной безопасности предприятия. М.: Городец, 2014. 352с.
4. Дунаев С. Доступ к базам данных и техника работы в сети. М.: Диалог МИФИ, 2014. 444 с.
5. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. СПб.: Университет МВД РФ, 2015. 226 с.
6. Штребе М. Безопасность сетей NT4. М.: Мир, 2011. 344 с.
7. Назаров С.В. Администрирование локальных сетей. М.: Финансы и статистика, 2015. 355 с.
8. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие. СПб.: Питер, 2008. С. 86–87.
9. Семененко В.А. Информационная безопасность. М.: МГИУ, 2010. 277 с.
10. Сычев Ю.Н. Основы информационной безопасности. М.: ЕАОИ, 2007. 300 с.