АКТИВНАЯ ЗАЩИТА ИСПОЛНЯЕМЫХ МОДУЛЕЙ ОТВЕТСТВЕННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

М.П. РЕВОТЮК, Т.А. ЖИРКО, А.П. КИШКЕВИЧ

Исполняемые модули ответственных систем обработки информации, представленные загрузочными файлами или файлами динамически подключаемых библиотек с открытым форматом PE (Portable Executable) в среде операционных систем Windows уязвимы для ряда угроз несанкционированного использования – копирования, дизассемблирования, модификации и запуска. Один из приемов защиты – связь процесса исполнения программного кода с сервисами группы AAA(Авторизация, Аутентификация, Аудит), рекомендуемых для создания серверных приложений.

Однако технологии создания серверных приложений не защищают файлы исполняемых модулей от дизассемблирования, трассировки или других угроз, реализуемых после получения файла. Кардинальным решением задач противодействия таким угрозам может быть криптографическая защита фрагментов кода.

Так как применение криптографии само по должно быть связано с состоянием аутентификации, то естественно образовать рекуррентную схему его связи с хотя бы одним предшествующим и остальными доступными для фиксации состояниями. Показано, что, используя криптографию с открытым ключом и реально доступные системные события, возможно до этапа инсталляции на ЭВМ построение динамической системы, привязанной к моменту аутентификации, функционирующей только при нулевых масках доступа к процессу лишь при предъявлении ключа зарегистрированного конечного пользователя.

Файл программы выступает как контейнер для хранения скрытых блоков кода. Преобразование кода выполняется в последний момент непосредственно перед использованием в проекции на память. Для проверки и установки в любой момент общесистемных условий целостности и безопасности на рабочей станции программа должна заимствовать на этапе инсталляции право использования строго регламентированных, но достаточных для самозащиты, административных привилегий.