Задача обеспечения информационной безопасности становится все более сложной и ресурсоемкой. Грамотно применяя облачные сервисы для информационной безопасности, клиенты получают выстроенные процессы защиты, возможность оперативно подключать или отключать услугу, оплачивая только тот объем сервисов, который необходим в конкретный момент времени.

УДК 355.4

А.Н. Шедько

СОЗДАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ

В настоящее время проблема обеспечения безопасности критически важных объектов информатизации (КВОИ) в каждом государстве приобретает все более актуальный характер. И в Республике Беларусь, и в Российской Федерации также уделяется значительное внимание этой проблеме. В частности, отмечается, что информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Также определяется, что угрозы информационной безопасности предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Создание системы безопасности (СБ) КВОИ предлагается рассматривать на примере стационарной цифровой автоматической телефонной станции (АТС) узла электросвязи сети общего пользования, обеспечивающей предоставление услуг в населенном пункте Республики Беларусь с численностью не менее 20 тыс. человек (далее – районный центр).

Объекты информатизации (ОИ) данной АТС размещены в пределах области действия одного комплекса безопасности (КЗ) и используются как критичные активы, так и обрабатывается общедоступная (открытая) информация, хотя одно или несколько средств вычислительной техники из совокупности имеют открытые каналы обмена информацией за пределами КЗ с другими ОИ. Так как при этом обеспечивается доступность и целостность критичных активов путем реализации мер,

направленных на предотвращение умеренного ущерба, то данным КВОИ присвоен класс В2-у.

Согласно перечню показателей уровня ущерба национальным интересам Республики Беларусь в социальной и демографической сферах в случае возникновения угроз различного характера в отношении ОИ (его составляющих элементов) уровень ущерба определяется с учетом того, что АТС размещена в районном центре, и оценивается как умеренный при прекращении функционирования на период от 48 до 72 ч более одной сети электросвязи (стационарная или сотовая подвижная электросвязь, передача данных, в том числе с доступом в сеть Интернет).

Если АТС в целом невозможно отнести к КВОИ, то приказом ее руководителя создается комиссия по отнесению отдельных ОИ АТС к КВОИ, утверждается ее председатель и состав. Комиссией составляется перечень ОИ АТС с их описанием (состав комплекса технических средств (средств электронной вычислительной техники), структура используемого программного обеспечения (перечень), общая функциональная схема (схема сети), наличие и характер взаимодействия с другими объектами и т. д.), который утверждается руководителем АТС. Для каждого из перечня ОИ АТС комиссия устанавливает отраслевые критерии отнесения ОИ к КВОИ методом экспертных оценок: определяются отраслевые критерии, перечень которых утвержден, и соответствие данных ОИ отраслевым критериям отнесения ОИ к КВОИ в соответствии с методикой, также утвержденной.

Руководителю АТС представляется отчет по результатам оценки соответствия ОИ АТС отраслевым критериям отнесения ОИ к КВОИ и составляются заключения о соответствии отдельных ОИ АТС отраслевым критериям отнесения их к КВОИ по утвержденной форме. В частности, к КВОИ комиссией может быть отнесена локальная информационная сеть АТС. Указанные заключения с описанием ОИ прилагаются к мотивировочному ходатайству и направляются по подчиненности в вышестоящую организацию для принятия решения об отнесении ОИ АТС к КВОИ.

При рассмотрении практических аспектов создания СБ КВОИ уже упоминалось о том, что в рамках создания СБ КВОИ разрабатывается и внедряется система менеджмента информационной безопасности.

Кардинальной мерой повышения защищенности сетей связи могла бы стать замена телекоммуникационного оборудования иностранного производства на «доверенное» отечественное, сертифицированное. Однако данное мероприятие сложное в организационно-техническом плане, требует больших затрат. Приемлемой альтернативой является оснащение существующего оборудования связи специализированными техническими средствами защиты.

В мировой практике в качестве основных технических средств для обнаружения и исключения злоумышленного воздействия через каналы внешнего доступа к телефонной сети используются защитные межстанционные экраны. С точки зрения алгоритма анализа и обработки информации экраны для АТС являются более сложными устройствами по сравнению с аналогичными решениями для компьютерных сетей.

УДК 004.087.5

А.И. Шемаров

СОЗДАНИЕ ИДЕНТИФИКАЦИОННЫХ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ ГИБРИДНЫХ МЕТОДОВ ЗАЩИТЫ НА ПРИМЕРЕ МИКРОКОНТРОЛЛЕРОВ ATMEL AVRMEGA

При создании идентификационных устройств существует проблема считывания кодов, записанных на этих устройствах, с последующей их эмуляцией. Получение кодов доступа для стандартных устройств, как правило, не вызывает значительных технических трудностей. Идентификационные карты на базе микроконтроллеров существенно усложняют задачу злоумышленников.

Проблема может быть решена с помощью гибридных методов защиты, не использующих записанный в идентификационной карте цифровой код, который является главной целью атаки злоумышленников. Это связано в первую очередь с доминированием цифровых технологий и математических криптографических алгоритмов. В качестве гибридной технологии целесообразно использовать объединение цифровых и аналоговых методов защиты информации. Применение таких гибридных методов заключается в создании и использовании дополнительного канала передачи кодированных аналоговых данных на базе физического интерфейса, применяемого для передачи цифрового кода. Передача аналогового кодированного сигнала сопровождается нарушением стационарных вероятностных характеристик аналоговых сигналов цифрового интерфейса. Реальный сигнал, несущий код, формируется в пределах допустимых отклонений физических параметров для конкретного интерфейса. Многообразие параметров физических сигналов, их вероятностные отклонения существенно усложняют задачу сканирования. Использование дополнительных каналов позволяет существенно упростить задачу идентификации оригинального устройства от его эмуляции, выполненной с помощью специальных технических средств.

Для иллюстрации метода рассмотрим возможную реализацию дополнительного канала передачи данных на базе широко распространенных микроконтроллеров фирмы ATMEL AVRmega. Эти контроллеры

используют RISC-архитектуру и отличаются развитой системой команд, позволяющих создавать эффективный быстродействующий код; имеют большое количество встроенных интерфейсов, которые можно использовать для решения практически любых задач при сопряжении микроконтроллера с другими средствами вычислительной техники и периферийными устройствами. Одним из наиболее широко используемых протоколов, применяемых для подключения разнообразных технических устройств как вычислительной техники, так и устройств связи является протокол универсального асинхронного приемника-передатчика UART (последовательного асинхронного стартстопного устройства). Протокол используется при создании таких распространенных интерфейсов, как RS-232, RS-485, Bluetooth (в режиме использования протокола RFCOMM), и многих других. В рассматриваемых микроконтроллерах используется от одного до четырех специализированных портов UART. Их имплементация осуществляется стандартным образом: путем совмещения функций выводов универсального порта со специализированным функционалом при использовании в качестве функционального устройства или интерфейса.

Современные инструментальные средства программирования используют их стандартным образом путем применения программных платформ (фрэймворков), определяющих структуру программной системы или программного обеспечения, облегчающего разработку и объединение разных компонентов большого программного проекта в единое целое для решения стандартизированной задачи.

Такой подход позволяет достаточно просто реализовать взаимодействие посредством выбранного интерфейса с предлагаемым набором стандартных функций, но не позволяет управлять им, так как это не предусмотрено производителем микроконтроллера. Для более ясного представления иллюстрируемого метода определимся с количественными параметрами. В качестве базовых параметров используем технические характеристики микроконтроллера ATmega128. Исходя из базовой частоты работы UART, равной 115 200 Гц (для получения требуемой скорости передачи данных эта частота подвергается аппаратному деления на целочисленный коэффициент), и максимальной частоты работы процессора этого типа, равной 16 МГц, определим частоту работы процессора как 115 200 × 138 = 15 897 600 Гц. По схеме передачи данных 115200-8-N-1 для передачи одного бита требуется 138 тактов работы микроконтроллера (за это время можно выполнить до 138 команд при использовании RISC-архитектуры), а при использовании схемы 9600-8-N-1 для передачи одного бита потребуется 1 656 тактов работы микроконтроллера соответственно. Наличие таких ресурсов производительности микроконтроллера позволяет выполнить формирование требуемой последовательности протокола без