Частично дополнительные функции безопасности можно реализовать путем использования штатных настроек ОС, установленных в АСФЗ, и применения организационных мероприятий.

В то же время в некоторых случаях невозможно использовать настройки ОС для реализации такого рода функций в связи с тем, что отсутствует необходимый уровень доверия к ОС (так как используются ОС иностранной разработки) и стойкости механизмов безопасности ОС. При применении организационных мероприятий также могут возникать отдельные сложности при контроле за их реализацией.

Многие необходимые дополнительные функции безопасности реализованы в общеприменяемых сертифицированных на соответствие требованиям по безопасности информации средствах защиты информации от НСД, таких как «Страж NT», «Аккорд-NT/2000», «Аура», «Secret-NET» и др.

Таким образом, для повышения уровня защищенности информации, обрабатываемой в АСФЗ, целесообразно использовать комплексный подход, т. е. прменять функции безопасности СПО совместно с функциями сертифицированных по требованиям безопасности информации средств защиты информации от НСД, что позволит снизить вероятность оказания негативных воздействий внутренним нарушителем на эффективность функционирования АСФЗ.

Д. А. Поладьев, С. И. Журин

СИСТЕМАТИЗАЦИЯ ПОРЯДКА ПРОВЕДЕНИЯ РАБОТ ПО СОЗДАНИЮ СЗИ В АСФЗ ВАЖНЫХ ОБЪЕКТОВ

Проблема обеспечения физической защищенности важных объектов (ВО) в настоящее время является особо актуальной. Эффективность работы современных автоматизированных систем физической защиты (АСФЗ) ВО зависит не только от квалификации обслуживающего персонала, качества и технических характеристик систем, но и от уровня защищенности информации, обрабатываемой в них.

Получив доступ к информации, обрабатываемой в АСФЗ ВО, потенциальный нарушитель может, например, внести изменения в функционирование системы, нарушить ее работоспособность или, обладая информацией из баз данных, осуществить несанкционированный доступ на объект. В связи с этим возникает необходимость создания систем защиты информации (СЗИ) АСФЗ ВО.

Работы по созданию СЗИ, обрабатываемой в АСФЗ ВО, должны состоять из следующих стадий:

а) стадия 1 — подразделяется на два этапа:

– первый — проведение предпроектного обследования АСФЗ. На данном этапе осуществляется сбор необходимых исходных данных о АСФЗ, таких как: функциональный состав АСФЗ, условия расположения и эксплуатации технических средств, порядок обращения персонала АСФЗ с защищаемой информацией и др.;

– второй — разработка «Аналитического обоснования требований к СЗИ, обрабатываемой в АСФЗ ВО». На данном этапе определяются: степень конфиденциальности информации, перечень технических средств, участвующих в обработке информации ограниченного доступа, возможные угрозы и каналы утечки информации; предлагается набор методов и средств защиты информации; предварительно оценивается стоимость создания СЗИ;

б) стадия 2 — подразделяется на два этапа:

– первый — разработка «Технического задания на создание СЗИ АСФЗ ВО». На данном этапе формируется набор мероприятий, которые должны быть реализованы в СЗИ АСФЗ, а также набор требований, которым должны отвечать проектируемые средства защиты информации;

– второй — разработка проектной (рабочей) документации на СЗИ. На данном этапе определяются наименования средств защиты информации, описываются детали размещения, монтажа и настройки средств защиты информации, описываются мероприятия, которые необходимо реализовать в АСФЗ, формируется детальная спецификация оборудования, а также оценивается стоимость проведения специальных работ, закупки, монтажа (установки), настройки средств защиты информации, а также реализации необходимых мероприятий;

в) стадия 3 — включает в себя 2 этапа:

– первый — закупка оборудования и программного обеспечения СЗИ, проведение специальных работ (при необходимости), поставка, установка (монтаж) и настройка проектируемого оборудования (программного обеспечения), а также реализация необходимых мероприятий;

– второй — проведение опытной эксплуатации СЗИ, внесение изменений в настройку средств защиты информации, изменение их местоположения, доработка организационно-режимных мероприятий (при необходимости);

г) стадия 4 — аттестация АСФЗ на соответствие требованиям по безопасности информации. Данная стадия включает в себя проверку выполнения необходимых функций средствами защиты информации и аудит достаточности мероприятий, предусмотренных проектной документацией.

Предлагаемое деление на стадии и этапы основано на практическом опыте создания СЗИ в АСФЗ и позволяет обеспечить высокую степень осведомленности заинтересованных лиц (в том числе исполнителей работ), четко регламентирует последовательность действий по созданию таких систем и, как следствие, повышает эффективность контроля выполнения работ в предметной области.

Таким образом, для построения эффективной СЗИ в АСФЗ необходимо выполнить полный цикл вышеуказанных работ. Исключение одного из этапов, несвоевременное их проведение или проведение в ином порядке может привести к несогласованности действий при выполнении работ и ошибкам при построении СЗИ, которые могут повлечь за собой излишние финансовые затраты на создание системы, утечку обрабатываемой в АСФЗ информации и снижение эффективности функционирования АСФЗ в целом.

А. С. Полякова

ИССЛЕДОВАНИЕ МОДЕЛЕЙ ОЦЕНКИ ОПТИМАЛЬНОГО ОБЪЕМА ИНВЕСТИЦИЙ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

В настоящий момент организации нерационально вкладывают средства в обеспечение ИБ: до 2/3 средств расходуются впустую. Возрастающая необходимость защиты информационных активов, а значит, и инвестирования в эту защиту, а также недостаточная разработанность принципов и рекомендаций по выбору оптимального объема инвестиций обуславливают потребность в исследовании экономических аспектов безопасности информации и выработки методики оценки оптимального уровня инвестиций в ИБ.