Д. А. Поладьев, С. И. Журин

СОВЕРШЕНСТВОВАНИЕ СЗИ АСФЗ ВАЖНОГО ОБЪЕКТА В ЧАСТИ ЗАЩИТЫ ОТ НСД ВНУТРЕННИМ НАРУШИТЕЛЕМ

В настоящее время актуальной проблемой является защита информации в современных автоматизированных системах физической защиты от несанкционированного доступа, осуществляемого внутренним нарушителем. Для качественного обеспечения защищённости информации рекомендуется использовать как функции безопасности специализированного программного обеспечения, под управлением которого функционируют современные автоматизированные системы физической защиты (АСФЗ), так и функции операционных систем, такие как идентификация и аутентификация пользователей, замкнутая программная среда, разграничение прав доступа пользователей и т. д. Такой комплексный подход позволит значительно повысить защищенность от внутреннего нарушителя.

В настоящее время актуальной проблемой при создании системы защиты информации (СЗИ), обрабатываемой в современных автоматизированных системах физической защиты, является проблема разработки методов защиты информации от несанкционированного доступа (НСД), осуществляемого внутренним нарушителем.

В частности, значительную трудоемкость составляют мероприятия по достоверному определению угроз, которые могут быть реализованы сотрудниками предприятия в отношении защищаемой информации, и негативных воздействий на эффективность функционирования АСФЗ.

Функции безопасности, направленные на предотвращение НСД, осуществляемого внутренним нарушителем, реализованы в продуктах специализированного программного обеспечения (СПО), под управлением которого функционируют АСФЗ.

СПО обычно выполняет следующие функции безопасности:

– идентификация и аутентификация пользователей при входе в СПО, а также регистрация входа и попыток входа в СПО (прием смены) и выхода из СПО (сдача смены);

– разграничение прав доступа пользователей к функциям настройки СПО, просмотру состояния и управлению оконечными устройствами (турникетами, техническими средствами охраны и др.) и регистрация изменения прав доступа пользователей СПО;

– контроль целостности СПО при его запуске;

– другие специфичные функции, характерные для отдельных версий СПО.

Помимо функций безопасности, выполняемых СПО, для повышения эффективности СЗИ в АСФЗ целесообразно реализовать дополнительные функции безопасности, такие как:

– идентификация и аутентификация пользователей при входе в операционную систему (ОС), а также регистрация входа и попыток входа в ОС и выхода из ОС;

– разграничение прав доступа пользователей к функциям настройки ОС, к томам, каталогам, файлам и регистрация изменения (попыток изменения) прав доступа пользователей в ОС;

– контроль целостности критичных системных файлов ОС;

– замкнутая программная среда (ограничение запуска программ, кроме необходимых);

– блокирование избыточных портов ПЭВМ и ограничение использования внешних (съемных) носителей информации;

– другие функции.

Отсутствие в АСФЗ такого рода функций может привести к совершению ошибочных действий персоналом АСФЗ или преднамеренных действий внутреннего нарушителя, что может повлечь за собой утечку, потерю или нарушение целостности защищаемой информации (например, баз данных) СПО, внесение изменений в настройки СПО, внедрение вредоносного программного обеспечения и, как следствие, может привести к снижению эффективности функционирования АСФЗ в целом.

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;