А. В. Мамаев

ПОВЫШЕНИЕ НАДЕЖНОСТИ СИСТЕМ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВНУТРЕННЕГО НАРУШИТЕЛЯ

Проблема внутренней безопасности организации остается крайне острой. Постоянное увеличение объемов конфиденциальной информации в организациях, изменение штата сотрудников, изменение бизнес-процессов — все это приводит к увеличению рисков утечки информации. Большие, сильно распределенные информационные системы крайне сложно контролировать службам безопасности [1]. Системы комплексной защиты информации от утечек, активно развивающиеся в последнее время, призваны для решения данной проблемы.

Однако не всегда компьютерная программа может сама распознать в действиях пользователя умышленное создание условий для утечки информации. Поэтому роль человека, сотрудника службы безопасности, остается крайне важной, именно для того, чтобы человек мог ее выполнить, система комплексной защиты информации от утечек должна максимально быстро и полно сообщать о подозрительных действиях пользователя [2]. Но как быть в том случае, когда мы имеем дело с умышленным инсайдом, когда сотрудник специально работает над задачей утечки информации?

Локально-вычислительная сеть, пользующаяся в качестве канала связи механизмами дистанционного мониторинга и управления, оказывается в пределах досягаемости инсайдера [3]. Это дает ему возможность создания временного интервала, когда наблюдение за атакуемой машиной будет снято. Таким образом, снижается надежность систем комплексной защиты информации от внутреннего нарушителя.

Для повышения надежности систем защиты, путем решения проблемы временной потери контроля за ПЭВМ, предлагается ввести в эксплуатацию дополнительный канал передачи. С помощью этого канала будет осуществляться дополнительный контроль повышенной надежности.

При выборе канала, альтернативного локально-вычислительной сети, важно помнить о том, что внутренний нарушитель, действующий умышленно, заранее продумывает свою атаку. Таким образом, необходимо обеспечить однозначное соответствие между работающей ПЭВМ и функционирующим каналом связи.

СПИСОК ЛИТЕРАТУРЫ:

1. *Ruppert B.* Protecting Against Insider Attacks. SANS Institute, 2009.
2. *Buenger W. Jr.* Developing an Insider Threat Mitigation Strategy. ISSA Journal, 2008.
3. *Лаврентьев Н. П., Мамаев А. В.* Анализ систем комплексной защиты информации от утечек с целью закрытия возможных уязвимостей // Безопасность информационных технологий. 2009. № 4. С. 117–119.