МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЦИФРОВЫХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ ВОЕННОГО НАЗНАЧЕНИЯ

В.А. Федоренко, М.Н. Лешкевич

Любая система имеет ряд уязвимостей. Рассмотрим основные способы воздействия нарушителя на цифровую систему передачи информации на примере цифровой радиорелейной системе связи. Данная система включает в себя: автоматизированное рабочее место (АРМ), модуль доступа, приемо-передающее устройство, антенну и, соединяющие это оборудование между собой, кабели.

Местами воздействия нарушителя и возможный результат его действий будут следующими:

а) получение доступа к АРМ, незащищенной операционной системе:

- изменение конфигурации управляемой системы;
- получение данных об характеристиках и установленных параметров аппаратуры;
- заражение вредоносным программным обеспечением;

б) место между модулем доступа и автоматизированным рабочим местом:

- ведение разведывательной работы за действиями системы;
- подставив модуль приема и анализатор принятого сигнала вводить пользователя АРМ в заблуждение и управлять модулем доступа;

в) имея выход к самому модулю доступа:

- подключить свое оборудование управления для действий, описанных выше;
- управление потоками, ввод/вывод их из эксплуатации;
- выведения из строя модуля для прекращения связи;

г) место посредника между внутренним и внешним блоком:

- получить мультиплексированную информацию потребителей сети;
- оборвать линию передачи между внутренним и внешним блоком;

д) получение доступа к месту соединения антенны и приемо-передающего устройства:

- оборвать линию передачи между антенной и приемо-передающим устройством;
- вести прослушивание [1, 2].

Литература

1. Утин Л.Л., Федоренко В.А., Масейчик Е.А. Военные системы радиорелейной связи. Минск: БГУИР, 2020. 160 с.

2. Эриксон Д. Хакинг: искусство эксплойта. СПб.: Питер, 2018. 496 с.