2.8 Проверка телефонов

Если телефонная система нецифровая, то при повешенной трубке аудиосигнал на проводах должен отсутствовать. У цифровых телефонных систем в линии может присутствовать мощный цифровой сигнал, похожий на шум. Можно отсоединить телефон от розетки, чтобы убедиться, что при этом шум в линии пропадает. Кроме того, если обнаруживается звуковой отклик при постукивании (например карандашем) по подключенному телефону с положенной трубкой, то это значит, что в телефоне установлено шунтирующее устройство. Некоторые типы телефонов остаются активными и при положенной трубке (особенно это касается телефонов с переговорными устройствами). Такой аппарат представляет прямую угрозу и его необходимо заменить.

При снятой трубке телефона аналоговой или гибридной системы хорошо прослушиваются все сигналы с микрофона (в гибридных системах используется аналоговый сигнал для переговоров и звонков и остальные 2...6 проводов для питания и цифрового управления).

Некоторые радиозакладки активируются только при снятой телефонной трубке, поэтому проверку следует проводить как при снятой, так и при повешенной трубке.

В заключение необходимо отметить, что следование приведенным выше рекомендациям позволит достичь успеха и повысить эффективность выполнения спецобследований помещений при условии, если они будут проводиться профессиональными специалистами.Это должны быть штатные сотрудники фирм, имеющих лицензии на услуги в сфере защиты информации.

ЛИТЕРАТУРА:

1. Каталог фирмы “Westinghause Audio Intelligence Devices ”, USA.

Поступила 29.11.2000 р.

УДК 681.3.004

Зуєв О.В., Хмелько Ю.М., Чирков Д.В.

КРИТЕРИЙ ОЦЕНКИ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Современные средства защиты информации (СЗИ) характеризуются множеством качественных показателей. Достижение требуемых значений качества по одним из показателей нередко сопровождается ухудшением качества по другим показателям. В таких условиях требуется объективная оценка качества СЗИ со стороны потребителя.

Качество СЗИ предлагается определять вероятностной мерой , значение которой должно соответствовать уровню доверия к СЗИ со стороны потребителя . Необходимо оценить обобщенные эксплуатационно-технические характеристики СЗИ, отражающие их свойство выполнить поставленную перед ними задачу с вероятностью не ниже заданой. Такая оценка может быть проведена в результате исследования целостности (Ц)СЗИ. Вероятность того, что исследуемое СЗИ окажется работоспособным в произвольный момент времени и проработает безотказно с этого момента в течении заданного интервала времени определяется непрерывностью обслуживания (НО) СЗИ.

Прежде чем производить оценку качества функционирования СЗИ необходимо определить какой уровень защиты требуется. Это защита при минимальных затратах и допустимом уровне ограничения видов СЗИ, либо защита при допустимых затратах и заданном уровне ограничений видов СЗИ, либо максимальный уровень защиты при необходимых затратах и минимальном уровне ограничений видов СЗИ.

Для определения уровня защиты можно воспользоваться вероятностной моделью СЗИ в соответствии с которой обработка информации на объекте осуществляется в условиях воздействия на информацию различных угроз [1,2]. Необходимо, в первую очередь, смоделировать поведение потенциального нарушителя, которое во многом определяет принцип построения СЗИ. На основании выбранного принципа построения СЗИ проводятся обследования условий функционирования объекта, средств обеспечения информационной деятельности, имеющие выход за пределы контролируемой территории, определения наличия и технического состояния средств обеспечения ТЗИ. Материалы обследования необходимо использовать при разработке модели угрозы СЗИ.

Оценку Ц и НО СЗИ целесообразно произвести на этапах испытаний и ввода в эксплуатацию,т. к. потребителю необходимо знание качества конкретных СЗИ с целью принятия решения о выборе предоставленного варианта СЗИ для дальнейшей их эксплуатации.Для оценки Ц и НО рассмотрим полную группу несовместных событий, представляющих собой вероятности возможных состояний СЗИ в соответствии с [2]:

$$P_1+P_2+P_3+P_4+P_5=1, \qquad (1)$$

где P_1- вероятность отказов, не устраняемых при проведении технического обслуживания СЗИ; P_2- вероятность отказов устраняемых при проведении ТО СЗИ; P_3=A- вероятность принятия ошибочного решения о неработоспособности работоспособного СЗИ по результатам контроля (вероятность ложного отказа);

P_4=B- вероятность принятия ошибочного решения о работоспособности неработоспособного СЗИ по результатам контроля (вероятность необнаруженного отказа); P_5- вероятность работоспособного состояния СЗИ.

Для эффективной работы СЗИ необходим постоянный контроль их параметров, с тем чтобы проводимый контроль постоянно обеспечивал необходимый уровень защиты. Возможности параметров этих комплексов необходимо определять еще на этапе их проектирования. При разработке систем контроля работоспособности и управления технической системой защиты информации объекта возникает задача нахождения компромисса между точностью и надежностью системы. Особенно это важно при создании систем активной технической маскировки объекта. При этом система должна создавать заградительную, шумовую или прицельную по частоте помехи, а так как по своей сути эти системы являются иерархическими сложными системами, то их анализ сопряжен с определенными трудностями. Так как с позиций технической защиты необходимо оценить информативность сигналов, которые снимаются с объекта, причем информативность сигнала тесно связана с надежностью и эффективностью противодействия.

На этапах испытаний и вводе в эксплуатацию СЗИ наиболее эффективным представляется метод оценки Ц и НО СЗИ на основе знания статистических данных об определяющих параметрах средств, допусках и погрешностях измерений параметров, а также надежностной статистики. В соответствии с полученными в [3] результатами целостность I определяется только вероятностью необнаруженного отказа B, т. е.

$$I=1-P_4=1-B=1-\beta_i[1-\prod_{i=1}^{n} P_i], \qquad (2)$$

где β_i- условная вероятность возникновения необнаруженного отказа по i-му контролируемому параметру; P_i- вероятность нахождения i-го контролируемого параметра в пределах допуска; n- количество контролируемых параметров.

Непрерывность обслуживания в соответствии с определением и соотношениями (1), (2) определяется следующим образом :

$$НО = P_5 = I - P_1 - P_2 - P_3 \qquad (3)$$

Вероятность ложного отказа P_3=А- определяется так [4]:

$$P_3 = P_i \cdot \alpha_i, \qquad (4)$$

где α_i - условная вероятность возникновения ложного отказа.

Для практических расчетов, предпологая закон распределения контролируемых параметров СЗИ и погрешностей их измерения нормальным для расчета вероятностей P_i, α_i, β_i используются выражения [4]:

$$P_i = 2\,\Phi(x_i) - 1;$$

$$\alpha_i = \frac{10 z_i}{n\sqrt{2\pi}} \sum_{m=1}^{n} e^{-\frac{U_m^2}{2}} \left[0{,}5 - \Phi_0\left(\frac{x_i - U_m}{z_i} \right) \right];$$

$$\beta_i = \frac{10 z_i}{n\sqrt{2\pi}} \sum_{m=1}^{n} e^{-\frac{U_m^2}{2}} \left[0{,}5 - \Phi_0\left(-\frac{x_i - U_m}{z_i} \right) \right]; \qquad (5)$$

где $\Phi_0(X_i)$-нормированная функция Лапласа, X_i-нормированное значение допуска на i-ый параметр СЗИ;

$$U_m = X_i - \frac{5Zi(n - m) + 2{,}5Zi}{n};$$

Z_i-нормированное значение средней квадратической погрешности измерения i-го параметра; m- номер члена суммы (параметра) ; n-предел суммы (количество контролируемых параметров).

Вероятности P_1 и P_2 определим в соответствии с методикой [2]:

$$p_1 = \frac{P_{св} P_{ва}}{P_{ав} P_{вс} + P_{св} P_{ва} + P_{ав} P_{св}}; \qquad (6)$$

$$P_2 = \frac{P_{ав} P_{вс}}{P_{ав} P_{вс} + P_{св} P_{ва} + P_{ав} P_{св}}$$

где $P_{ав}, P_{вс}, P_{св}, P_{ва}$ - переходные вероятности , определяемые по формулам

$$P_{ав} = \frac{t_п}{T_A}, \quad P_{вс} = \frac{N_c t_п}{T - N_A T_A - N_c T_c};$$

$$P_{с\,в} = \frac{t_п}{T_c}, \quad P_{ва} = \frac{N_A t_п}{T - N_A T_A - N_c T_c}.$$

где $t_п$- время поиска отказа при проведении ТО СЗИ; T_A - время восстановления СЗИ после отказов 1-го рода, Т- интервал наблюдения; N_c- количество отказов 2-го рода за интервал наблюдения Т , N_A- количество отказов 1-го рода за интервал Т, T_c- время устранения отказа 2-го рода.

Этап ввода СЗИ в эксплуатацию характеризуется повышенным уровнем интенсивности отказов. Отказы на ранних стадиях эксплуатации могут возникать вследствие наличия ошибок проектирования, изготовления, а также нарушения правил эксплуатации. Непрерывность обслуживания СЗИ в общем случае, определяется уровнем надежности СЗИ и расчет НО, особенно на ранних стадиях эксплуатации , требует сбора параметрической и надежностной статистики в соответствии с выражениями (2-6).

На этапе ввода в эксплуатацию СЗИ необходим контроль работоспособности и управления технической защиты информации, который может осуществляться путем создания систем активной технической маскировки объекта. Учитывая, что для средств технической защиты информации применяются различные средства (технические, программные, элементы строительных конструкций), то во время эксплуатации необходимо осуществлять специальный контроль такими средствами как индикаторами и обнаружителями угроз, контроля эффективности ТЗИ, программными средствами контроля эффективности ТЗИ.

При анализе СЗИ требуется индивидуальный подход к решению задач выбора и оптимизации контролируемых параметров, учитывающий особенности структурно-функциональных схем исследуемых средств, взаимосвязи параметров, режимы работы, расположение точек контроля, наличие штатной контрольно-измерительной аппаратуры. Полнота и достоверность исходной статистики в значительной мере влияют на эффективность оценки качества функционирования СЗИ.

Обозначим через m количество доступных для измерения параметров СЗИ, контроль которых безусловно обеспечивает равенство единице методической составляющей достоверности контроля, т.е. в этом случае идеальная модель СЗИ исчерпывающим образом описывает реальное средство. Известно [4], что методическая составляющая достоверности контроля является монотонно возрастающей функцией количества контролируемых параметров n, ассимптотически стремящейся к единице при его увеличении. Однако, при этом возрастают стоимость и время контроля. Таким образом, рациональный выбор совокупности контролируемых параметров должен обеспечить высокий методический уровень контроля при приемлемых стоимостных и временных затратах.

С учетом требований обеспечения заданного уровня целостности, определяемого условными вероятностями ошибок β_i в соответствии с выражением (2), выбранная совокупность параметров n будет оптимальной, при условии, что контроль этих параметров ($n \le m$) обеспечит выполнение условия

$$\beta(n) \le \beta_з, \qquad (7)$$

где $\beta(n)$ - условная вероятность необнаруженного отказа СЗИ при контроле n параметров из общего количества m; $\beta_з$ – заданное предельно допустимое значение β, вызванное неполнотой контроля параметров при минимальных стоимостных затратах.

Следовательно, для решения задачи выбора контролируемого количества параметров n рекомендуется определить значения Pi для каждого из параметров в соответствии с выражением (5), расположить параметры в порядке убывания их значений P_i, а затем последовательно отобрать такое их количество $n \leq m$, при котором удовлетворяется условие (7). Данный подход позволит избирательно оценить влияние каждого параметра на общий уровень целостности СЗИ.

Объективность анализа и обработки надежностной статистической информации, получаемой в результате наблюдения за СЗИ в процессе подконтрольной эксплуатации, существенно зависит от полноты сведений о каждом случае нарушения функционирования СЗИ.

В процессе наблюдений необходимо обеспечить фиксацию следующей информации:

- общая наработка изделия Т и время работы от момента предыдущего нарушения;
- количество отказов 1-го рода N_A и 2-го рода N_c за интервал наблюдения Т;
- место нарушения, отказавший элемент или узел;
- причина нарушения;
- последствия нарушения (полное нарушение функционирования или частичное и по каким именно функциям);
- вид нарушения (поломка, износ, уход параметра за пределы допусков, сбой и т.д.);
- время поиска отказа (нарушения) t_n;
- способ устранения нарушения (замена элемента, регулировка и т.д.);
- время восстановления СЗИ после нарушения функционирования T_A;
- время устранения нарушения T_c;
- условия окружающей среды в момент нарушения функционирования (температура, влажность и т.д.).

При отказе полученных статистических данных выявленные отказы необходимо классифицировать по причине и характеру возникновения:

- отказы, возникшие в результате нарушения норм конструирования (конструктивные);
- возникшие в результате нарушения правил и условий эксплуатации (эксплуатационные);
- возникшие в результате нарушения установленного процесса изготовления и ремонта (производственные);
- отказы комплектующих элементов.

При обработке надежностной статистики учитываются все отказы, за исключением эксплуатационных и устраненных по бюллетеням доработок.

В процессе экспериментальной оценки надежности определяются показатели типа наработки либо типа вероятности .

При определении показателей типа наработки непосредственно наблюдаемыми случайными величинами являются случайные интервалы- наработки до отказа, между отказами, до предельного состояния, времени восстановления и т.д. При определении показателей типа вероятности непосредственно наблюдаемыми случайными величинами являются числа событий в испытаниях СЗИ- число отказов, число восстановлений, число предельных состояний и т.д.

Для оценки показателей надежности необходимо знать вид функции распределения наблюдаемой случайной величины. Если вид функции распрелеления известен априорно, то задача статистической обработки сводится непосредственно к получению оценок показателей надежности с учетом вида функции распределения. Если вид функции распределения наблюдаемой случайной величины неизвестен, то на основании

предварительного анализа полученной информации необходимо принять гипотезу о виде функции распределения.

Имеет смысл разделение отказов на устойчивые и отказы сбойного характера, т.к. сложные СЗИ при частичных отказах, характерных для дискретной техники, могут функционировать с различными уровнями эффективности. Устойчивые отказы устраняются с помощью ремонтных операций, отказы сбойного характера могут быть устранены путем исключения искаженной информации без проведения ремонтных операций (поворотный пуск программы контроля, переход на резервный модуль при условии работоспособности основного и т.д.).

Наличие указанных разновидностей отказов позволяет говорить в общем случае о двух составляющих надежности: субстанциональной, обусловленной устойчивыми отказами аппаратуры и функциональной, обусловленной отказами сбойного характера.

Для оценки качества функционирования СЗИ, с учетом устойчивых и сбойных отказов, предлагается наряду с оценкой наработки на отказ по статистическим данным о наработке и количестве отказов, определять вероятность безотказного включения $P_{вкл}$ (вероятность того, что СЗИ, находящееся в выключенном состоянии, после включения и контроля работоспособности окажется в работоспособном состоянии) и наработку на отказ сбойного характера $T_{осб}$:

$$P_{вкл}=(N_{вкл}-n_{вкл})/ N_{вкл},$$

$$T_{осб}=T_{\Sigma}/ n_{осб},$$

где $N_{вкл}$ - общее количество включений СЗИ; $n_{вкл}$ - число устойчивых отказов, зарегистрированных при включении; T_{Σ} - суммарное время работы СЗИ; $n_{осб}$ - количество сбоев, зарегистрированных за время T_{Σ}.

Оценка качества функционирования СЗИ по критериям Ц и НО на этапах их испытаний , ввода в эксплуатацию и сравнительной оценки эффективности позволит сравнить СЗИ , характеризуемые множеством индивидуальных показателей , по уровню доверия к ним со стороны потребителя , выбрать оптимальные СЗИ в рамках поставленных потребителем задач.

Список литературы

1. Браиловский Н.Н., Хорошко А.В., Хорошко В.А., Чирков Д.В. Взаимосвязь между информативностью и эффективностью в системах технической защиты. //Захист інформації. - 2000.-№1.-с.15-18.

2. Провести исследование по оценке стабильности и надежности работы опытного образца " Плацдарм-1 Н". Заключительный отчет НИР № 768-В 90. КИИГА, Новиков В. С. -Киев, 1990г.-132 с.

3. Хмелько Ю. М. , Зуев А. В. Анализ целостности наземного оборудования микроволновой системы посадки.Защита информации- Киев: КМУЦА, 1995 г.-с.102-106.

4. Белоконь Р. Н., Скрипник В. М. Основы теории контроля -Минск; 1987г--152 с.

Поступила 23.11.2000 р.