$t_{вер}$, t_{max}, - минимальное, вероятное и максимальное время выполнения элементарной операции соответственно; M_t, D_t – статистические показатели математического ожидания и дисперсии; $\Phi_0(z)$ – функция Лапласа. Расчет вероятности реализации НСД осуществляется по формуле

$$P(t \le T) = 0.5 + \Phi_0\left(\frac{T - M_t}{t}\right),$$

где $M_t = \sum_{i=1}^{n} \frac{t_{\min} + t_{вер} + t_{\max}}{6}$; $D_t = \sum_{i=1}^{n} \frac{(t_{\max} - t_{\min})^2}{36}$; $\Phi_0(z) = \frac{1}{\sqrt{2\Pi}} \int_0^z e^{-\frac{z^2}{2}} \partial z.$

Пример решения задачи.

В результате проведенного исследования была выявлена последовательность элементарных операций по вскрытию. При этом использовались как механизмы работы сетевых анализаторов, так и реализовывались варианты известных атак. Время выполнения элементарных операций определялось экспериментальным путем. Расчеты показали, что вероятностные характеристики осуществления НСД к информации, защищенной МЭ, за время T=100 часов имеют следующие значения:

Таблица 1

№	Межсетевой экран	Стоимость		*P*
		Базовый	Корпоративный	
1	ISA Server	≈ $1500	≈ $6000	0.632
2	Enterprise Firewall 7.0	≈ $2500	≈ $7000	0.516
3	FireWall-1	≈ $3000	≈ $10000	0.358
…	…	…	…	…

С учетом результатов проведенного анализа была выработана стратегия построения защищенной среды функционирования РИС на основе корпоративных МЭ FireWall-1 и ISA Server.

Естественно, что данный метод не учитывает ряд существенных характеристик МЭ, которые могут быть серьезным аргументом при осуществлении выбора. Например, использование собственной аппаратной и операционной среды, наличие сертификата ГТК, методы реализации механизмов фильтрации, уровень организации виртуальных сетей и т.д. Однако представляется, что он может быть одним из основных инструментариев при комплексном анализе возможности реализации конкретной схемы РМЭ и экономической эффективности ее применения.

Библиографический список

1. *Мельников В.В.* Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997

2. *Хубаев Г.Н.* Безопасность распределенных информационных систем: обеспечение и оценка//Известия ВУЗов. Северо-Кавказский регион. Технические науки. Спецвыпуск. – Ростов-на-Дону, 2002

Ш.А Заргаров, А. Ахмаджонов
Узбекистан, г. Ташкент, Институт Кибернетики

О СРЕДСТВАХ ЗАЩИТЫ ЦИФРОВОЙ И АНАЛОГОВОЙ ИНФОРМАЦИИ

В настоящее время обслуживание пользователей компьютеров всеболее происходит в форме удаленного доступа к ресурсам распределенной информационной системы, к числу которых относится телекомуникационные и компьютерные сети. В силу этого обстаятельства увеличивается возможность утечки инфор-

мации. В связи с этим возрастает роль создания эффективных мер защиты информации.

Так как процессы защиты информации подвержены сильному влиянию случайных факторов, методы классической теории систем оказываются практически непригодными для решения задач обеспечения информационной безопасности [1]. Кроме того, отсутствует статистика функционирования реальных систем защиты информации. Поэтому на первый план выходит необходимость разработки эвристических методов защиты информации. При проектировании эффективных систем защиты информации необходимо по возможности стремиться создавать оптимальные механизмы обеспечения защиты информации с учетом требуемого уровня информационной безопасности.

Разработка эффективных мер предотвращения потециальных угрозпередаваемым данным или компьютерной (цифровой) и речевой (аналоговой) информации, программных и технических средств их реализации
со сведением к минимуму возможного при этом ущерба осуществляется в основном в теоретическом плане. Последние программные и технические разработки в этой области, естественно, отсутствуют на информационном рынке, а в продажу поступают средства, которые являются пройденным этапом или не представляют собой стратегической ценности (как, например, программы анализа защищенности и программы proxy серверов). Стоимость этих средств довольно высока. Кроме того, и это самое главное, каждая страна должна сама обеспечивать закрытость соответствующей своей информации, т.е. ее защиту таким образом, чтобы нарушитель не мог ею мог ею воспользоваться. Эти обстоятельства определяют необходимость разработки "своих" целенаправленных и практически действенных средств защиты информации с учетом потенциальных угроз и обеспечения необходимых уровней информационной безопасности в зависимости от затрат на нее.

Количественная оценка возможного ущерба от реализации той или иной угрозы цифровой информации ведется в разработке и объединении методов определения вероятности реализации угроз и показателей возможного ущерба при этапе.

Для решения задачи оптимизации выбора средства защиты цифровой информации для обеспечения необходимого уровня информационной безопасности в информационных системах целесообразно разработать обобщенную структуру системы защиты информации, которая позволит легче и более объективно создать соответствующую математическую модель, а также программу, реализующую такой подход. Решение задачи создания устройств защиты утечки информации от электромагнитного излучения компьютеров и защиты речевой (аналоговой) информации предлагается осуществить с помощью разработки принципов действия и электронных схем этих устройств прием уменьшения отношения сигнал (помеха с учетом реальных помех).

Для решения указанных задач представляется необходимым решить следующие задачи:

- анализ возможных видов (характера) передаваемых в информационных системах сообщений;
- определение множества угроз информации и их классификация;
- научно обоснованный выбор методики предотвращения угроз с учетом экономичности защиты информации.

Библиографический список

1. *Малюк А.А.* Современные проблемы защиты информации и пути их решения.-http ://www tsure.ru / University / Faublties/Fib/bit/rus/stm 2806/ 1.htm. 2002. 8с.