С. И. Боридько, В. С. Попов

ОЦЕНКА УЯЗВИМОСТИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ ПО ОТНОШЕНИЮ К ДЕЙСТВИЯМ НАРУШИТЕЛЯ

В настоящее время оценка уязвимости информационно-вычислительных систем (ИВС) к действиям нарушителя сводится к оценке характеристик конкретного программного и/или аппаратного обеспечения, протоколов передачи данных и т. д. Все эти оценки проводятся инструментальными средствами и направлены на определение конкретных уязвимостей в ИВС. Таким образом, общая оценка уязвимости ИВС к действиям нарушителя (как внутреннего, так и внешнего) проводится только экспертным путем, а зачастую вообще не проводится. В связи с этим для оценки эффективности мероприятий по защите ИВС необходимо ввести формальные показатели уязвимости ИВС в целом.

Условная уязвимость ИВС к действиям нарушителя оценивается вероятностью $Q_{дн}$ достижения цели действий нарушителя в отношении рассматриваемой ИВС, а показателем защищенности ИВС является вероятность $P_{дн}$ пресечения действий нарушителя в ее отношении. Значение показателя защищенности для рассматриваемой ИВС зависит от характеристик программных и аппаратных средств, обеспечивающих функционирование ИВС, а также используемого для защиты ИВС от несанкционированных действий нарушителя. Также можно принимать во внимание возможность подключения к общедоступным сетям, оснащенность и подготовленность администраторов безопасности, физико-географические условия размещения узлов ИВС.

Можно считать, что показателем защищенности ИВС (эффективности ее подсистемы защиты) является

$$P_{дн} = P(\tau = 0/A),$$

где τ — коэффициент прохождения (пропускания), который можно представить бинарной функцией $\tau = \begin{cases} 0, & h > R, \\ 1, & h \le R. \end{cases}$, например, при защите от несанкционированного доступа внешнего нарушителя в зависимости от используемых средств защиты информации (СЗИ) и средств вторжения, применяемых нарушителем, τ принимает значение 0 или 1 (то есть реализован НСД или нет); A — совокупность характеристик факторов, влияющих на защищенность ИВС (возможностей администраторов безопасности, средств подсистемы защиты и т. д.).

Вероятность достижения цели действий нарушителя в отношении ИВС, оснащенной средствами защиты информации, определяется также соотношением

$$P_{дн} = P(T > O),$$

где T — возможности нарушителей, описываемые их количеством, оснащенностью, обученностью и способами действий (моделью внешнего нарушителя); O — соответствующие технические и человеческие возможности подсистемы защиты ИВС.

Приближенная оценка уязвимости ИВС по степени ее оснащенности СЗИ. Выделим из вектора A характеристик факторов, влияющих на защищенность ИВС, ведущий фактор — степень обеспеченности СЗИ, препятствующими осуществлению противоправных действий и позволяющими повысить вероятность их пресечения. Для определения этапов количественной оценки показателя защищенности (уязвимости) по степени обеспеченности СЗИ за основу можно взять методику из [1] и, доработав ее, использовать следующие этапы:

- количественная оценка фактической степени α обеспеченности объекта СЗИ;
- установление модели зависимости $P_{дн}(\alpha)$;
- расчет с помощью указанной модели по фактической степени обеспеченности объекта СЗИ показателя защищенности объекта.

Оценка степени обеспеченности объекта СЗИ. Рациональная (на рассматриваемом временном интервале с учетом существующих экономических, временных и иных ограничений) комплектация СЗИ для объекта закрепляется в форме требуемой (планируемой либо рекомендуемой) обеспеченности.

В качестве количественного показателя обеспеченности используется степень обеспеченности объекта СЗИ по отношению к требуемой (планируемой или рекомендуемой):

$$\alpha = \frac{N}{N_m},$$

где $N = \sum_{k=1}^{r} N_k$ — фактическое количество размещенных на объекте СЗИ; $N_m = \sum_{k=1}^{r} N_{mk}$ — требуемое количество указанных средств (количество средств, рекомендованных или запланированных к установке на объекте); $N_{тk}$ — требуемое количество СЗИ k-го типа на объекте.

Пусть c_k — нормированная на единицу значимость (вес) k-го типа СЗИ в обеспечении защищенности объекта, $\sum_{k=1}^{r} c_k = 1$. Тогда степень обеспеченности объекта СЗИ с учетом относительной значимости отдельных типов средств защиты можно определить по формуле:

$$\alpha = \frac{\sum_{k=1}^{r} c_k N_k}{\sum_{k=1}^{r} c_k N_{mk}} \times 100\% \qquad (1)$$

Коэффициенты относительной значимости (веса) отдельных типов СЗИ в первом приближении пропорциональны их стоимости. Поэтому значимость (вес) k-го типа СЗИ определяется по формуле:

$$c_k = \frac{C_k}{\sum_{k=1}^{r} C_k}, \qquad (2)$$

где C_k — стоимость (цена) СЗИ k-го типа.

Рассмотрим пример: в рамках некоторой программы повышения защищенности рассматриваемая ИВС должна быть оснащена СЗИ двух типов в следующей комплектации: тип 1 — 2 шт. (цена C_1 составляет 100 тыс. руб./шт.); тип 2 — 1 шт. (цена C_2 — 300 тыс. руб./шт.).

Фактически установлены СЗИ лишь первого типа. Какова степень обеспеченности объекта СЗИ?

Определим по (2) значимость каждого из двух типов СЗИ, планировавшихся к установке в ИВС:

$$C_1 = \frac{C_1}{C_1 + C_2} = \frac{100}{100+300} = 0{,}25, \quad C_2 = \frac{300}{100+300} = 0{,}75.$$

Тогда по (1) получим:

$$\alpha = \frac{c_1 N_1 + c_2 N_{m2}}{c_1 N_{m1} + c_2 N_{m2}} \times 100\% = \frac{0{,}25 \times 2 + 0{,}75 \times 0}{0{,}25 \times 2 + 0{,}75 \times 1} \times 100\% = 40\%.$$

Установление модели зависимости $P_{дн}(\alpha)$. Пусть α_0 — значение степени обеспеченности объекта СЗИ рассматриваемых типов на момент начала реализации мероприятий по оснащению средствами защиты.

Будем полагать, что зависимость $P_{дн}(\alpha)$ на интервале $(\alpha_0, 1)$ является линейной (Рис. 1). Значение $\alpha = 1$ соответствует случаю, когда фактическая степень обеспеченности СЗИ соответствует требуемой (планируемой или рекомендуемой).

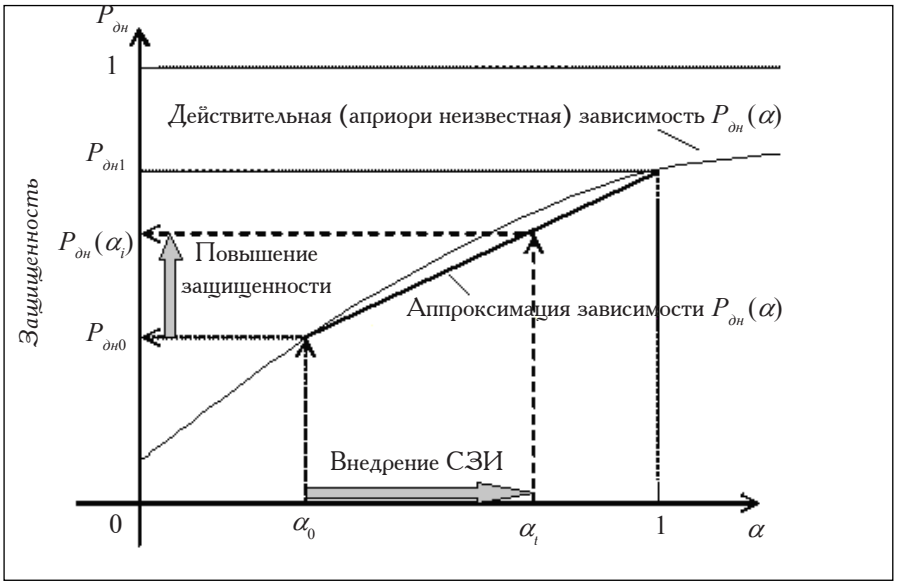

Рис. 1. Зависимость защищенности ИВС от степени ее обеспеченности СЗИ

Для калибровки модели зависимости $P_{дн}(\alpha)$ с помощью одного из имеющихся программных средств рассчитывают ее параметры:

$P_{дн}(\alpha = \alpha_0) = P_{дн0}$ — начальное (до начала выполнения мероприятий) значение показателя защищенности объекта;

$P_{дн}(\alpha = 1) = P_{дн1}$ — значение показателя защищенности объекта для требуемого уровня его обеспеченности СЗИ.

Значение показателя защищенности при некоторой обеспеченности объекта СЗИ

$$P_{дн}(N_1, \ldots, N_k, \ldots, N_r/A),$$

где A — вектор значений влияющих факторов, N_k — фактическое число установленных СЗИ k-го типа, r — число типов СЗИ, планировавшихся (рекомендовавшихся) к установке на объект, оценивается с помощью известных программных средств. При этом для решаемой задачи можно ограничиться оценкой лишь отдельных составляющих показателя $P_{дн}$, учитывающих влияние СЗИ, в частности, вероятности обнаружения нарушителя при его движении к цели защиты, вероятности верного определения масштаба вторжения и своевременного принятия решения на реагирование, технической оснащенности ИВС, влияющей на скорость вторжения нарушителя, — без учета действий администраторов безопасности.

Тогда для $\alpha \in (\alpha_0, 1)$ будет иметь место приближенная зависимость

$$P_{дн}(\alpha) = P_{дн0} + (P_{дн1} - P_{дн0})\frac{\alpha - \alpha_0}{1 - \alpha_0},\ \alpha_0 \le \alpha \le 1.$$

В частном случае при $\alpha_0 = 0$ получим:

$$P_{дн}(\alpha) = P_{дн0} + (P_{дн1} - P_{дн0})\ \alpha.$$

При невозможности оценки параметров $P_{дн0}$ и $P_{дн1}$ (отсутствии программных средств, необходимых исходных данных по ИВС или системе ее защиты) принимается допущение, что защищенность ИВС от действий нарушителя пропорциональна степени ее оснащенности СЗИ (т. е. линейно зависит от степени оснащенности). Тогда при $\alpha = 0$ $P_{дн} = 0$, а при $\alpha = 1$ $P_{дн} = 1$. В этом случае

$$P_{дн}(\alpha) = \alpha,$$

т. е. защищенность объектов полностью определяется их обеспеченностью СЗИ.

Расчет показателя уязвимости ИВС. Для достигнутой в процессе выполнения мероприятий по повышению защищенности на момент t оценки фактической степени обеспеченности ИВС

СЗИ α_l с помощью полученной модели рассчитывается фактическая защищенность ИВС $P_{дн}(\alpha_l)$. Показатель уязвимости ИВС рассчитывается по формуле

$$Q_{дн}(\alpha_l) = 1 - P_{дн}(\alpha_l).$$

Таким образом, рассчитав показатель уязвимости ИВС, используя метод оценки уязвимости ИВС по степени ее оснащенности СЗИ, можно сделать вывод о фактической защищенности ИВС в процессе выполнения мероприятий по защите ИВС. Это позволяет делать выводы об эффективности внедрения или модификации подсистемы защиты. Безусловно, разработанный метод не отменяет необходимость использования инструментальных средств анализа уязвимостей, конкретных программных и/или аппаратных средств, а только дополняет их, в качестве обобщенного показателя уязвимости ИВС.

СПИСОК ЛИТЕРАТУРЫ:

1. *Боридько С. И., Тихонов Б. Н.* Модели управления состоянием критически важных объектов: монография. М.: МИНИТ ФСБ России, 2006.
2. *Домарев В. В.* Безопасность информационных технологий. Системный подход. К.: ООО «ТИД Диа Софт», 2004.

А. Н. Голубинский

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ РЕЧЕВОГО СИГНАЛА, ОСНОВАННАЯ НА АППРОКСИМАЦИИ СПЕКТРА НАБОРОМ ПОСТОЯННЫХ СОСТАВЛЯЮЩИХ В СООТВЕТСТВУЮЩИХ ПОЛОСАХ ЧАСТОТ

Введение

В современных системах безопасности и информационных системах можно выделить две важные научно-практические задачи — идентификация и верификация личности [1]. При верификации (подтверждении) личности человека требуется установить его соответствие данному эталону, приняв одно их двух решений: заявитель является тем, за кого он себя выдает, или не является. При идентификации (установлении) личности человека необходимо выбрать из имеющейся базы данных эталонов тот эталон, на который заявитель максимально похож, при этом нужно принять решение: заявитель наиболее похож на конкретную персону (чей эталон находится в базе данных) или заявитель не соответствует ни одной из персон (имеющихся в базе данных).

В последнее время все более часто находят применение биометрические системы аутентификации (верификации и идентификации) личности [1], принцип работы которых основывается на анализе различных персональных физиологических характеристик людей, таких как форма и размеры руки, отпечаток пальца, голос, параметры зрачка и сетчатки глаза, форма и размеры лица и т. д. Одним из перспективных способов аутентификации личности является подтверждение или установление личности по голосу на основе речевого сигнала человека [1].

Следует отметить, что существуют различные методы построения моделей речевых сигналов [2, 3]. Приведем пять основных подходов к созданию математических моделей речевых сигналов, заданных функциональной зависимостью отсчетных значений модели от времени: