УДК 004.056.5(045)

Журиленко Б.Е., Николаева Н.К., Пелих Н.С.

ОЦЕНКА СТОЙКОСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ВО ВРЕМЕНИ

Получено выражение и метод расчета вероятности взлома технической защиты информации (ТЗИ) во времени. Полученное выражение подчиняется закону геометрического распределения вероятностей взлома, позволяет учитывать статистические или сертификационные данные в исследованиях по защищенности информации во времени и оценить эффективность используемого ТЗИ.

Ключевые слова: техническая защита информации, вероятность взлома ТЗИ, закон геометрического распределения вероятности взлома, критерий защищенности ТЗИ, эффективность использования ТЗИ.

Введение. Для защиты секретной, конфиденциальной и “ноу-хау” информации от утечки по техническим каналам необходимо создавать комплекс технической защиты информации (КТЗИ). Определяемые в процессе моделирования значения характеристик защиты должны соответствовать значениям, которые будут или могут иметь место в процессе функционирования реальной системы защиты. В литературе [1-2] приводятся методы расчета рисков, финансовых затрат и оценки эффективности защиты информации, однако, кроме работы [3] нет моделей, с помощью которой можно было бы оценить деградацию комплекса технической защиты информации во времени, так как в процессе использования эта защита устаревает не только в моральном, но и техническом плане.

В работе [3] зависимость стойкости КТЗИ от времени дается в параметрическом виде и только до сертифицированного времени защиты. После этого сертифицированного времени сложно дальше проводить аналитические исследования устойчивости КТЗИ к возможности взлома. В реальных условиях вероятность защищенности информации возможна и после сертифицированного времени защиты.

В теории оценки надежности радиоэлектронной аппаратуры [4] существуют два подхода к определению закона распределения вероятности отказов. Первый основан на подборе наиболее подходящей функции для описания эмпирического распределения. В этом случае используются различные критерии правдоподобия. Такой подход возможен, но он не отражает физической сущности закона распределения. В связи с этим такой подход не может быть признан оптимальным.

Второй подход основан на том, что каждому из возможных законов распределения вероятности отказов соответствуют вполне определенные условия. Тогда для вероятностей отказов не нужно искать эмпирические законы распределения, а можно использовать известные [5].

Таким образом, в работе [3] зависимость распределения взломов ТЗИ соответствует первому способу оценки надежности, когда определяется эмпирическое распределение вероятности взлома, получаемое из теории игр.

Для аналитических исследований необходимо использовать известные распределения вероятностей наиболее приближенные к физическим процессам, которые можно было бы корректировать по результатам экспериментальных исследований.

В связи с этим целью работы было получение метода оценки стойкости ТЗИ во времени с использованием известных распределений вероятностей.

Основная часть. Пусть t_0 – время с момента создания технической защиты информации (ТЗИ), до момента ее конкретного использования, t – текущее время в течение которого осуществляется защита, $p'(t)$ – вероятность защищенности ТЗИ во времени.

Определим риски защищенности ТЗИ во времени, как

$$(t_0 + t)\cdot p'(t) = f(t), \qquad (1)$$

где $f(t)$ - произвольная положительная функция.

Анализируя выражение (1), можно сказать, что для обеспечения защиты ТЗИ функция рисков защищенности $f(t)$ при увеличении времени защищенности t должна быть хотя бы постоянной. Если $f(t)$ со временем будет уменьшаться, то используемая ТЗИ является не эффективной и ее необходимо поменять на другую защиту. В случае если $f(t)$ увеличивается со временем, то такая ТЗИ является более эффективной.

Таким образом, если ТЗИ не сертифицирована во времени, то для оценки временной деградации ТЗИ необходимо брать случай $f(t) = const$, который обеспечивает минимально возможную защиту во времени.

В то же время выражение (1) может служить критерием эффективности использования ТЗИ во времени. Если известны вероятность $p'(0)$ при $t=0$ и вероятность $p'(t_1)$ через некоторое время $t = t_1$, то подставляя эти значения в выражение (1) и сравнивая полученные результаты $f(t) \geq f(0)$, можно сделать заключение об эффективности использования ТЗИ. Условие $f(t) = const$ соответствует минимально необходимым рискам ТЗИ.

Из (1) вероятность защищенности при $f(t) = const$ будет

$$p'(t) = \frac{const}{t_0 + t}. \tag{2}$$

Определим $const$ из начальных условий. При $t=0$ вероятность защищенности $p'(0)=1$. Отсюда

$$p'(0) = \frac{const}{t_0} = 1; \quad const = t_0. \tag{3}$$

Следовательно, вероятность защищенности ТЗИ во времени будет

$$p'(t) = \frac{t_0}{t_0 + t}. \tag{4}$$

Если за время t_0 вероятность защищенности ТЗИ морально или технически устарели в α раз, то можно записать

$$p'(t) = \frac{\alpha \cdot t_0}{t_0 + t}, \qquad \text{где } 0 \leq \alpha \leq 1. \tag{5}$$

При $\alpha=0$ ТЗИ настолько устарела, что защита полностью отсутствует и ее применение бессмысленно. Случай $\alpha=1$ возможен, если применение ТЗИ осуществляется сразу же после ее создания. Практически величина α – защищенности системы должна быть ближе к единице, иначе использование такой ТЗИ будет не эффективно. Пределы наиболее эффективного значения и возможного изменения величины α требуют дополнительных комплексных исследований.

Определим вероятность взлома во времени

$$p(t) = 1 - p'(t) = 1 - \frac{\alpha \cdot t_0}{t_0 + t} = \frac{(1-\alpha)\cdot t_0 + t}{t_0 + t}. \tag{6}$$

Выбираем независимость вероятности взлома от результатов предыдущих попыток и, если с очередной попытки взлом не произошел, то считаем, что вероятность взлома используемой защиты остается той же. Такое распределение попыток взлома будет подчиняться геометрическому закону распределения вероятностей [5].

Вероятность события взлома на m – той попытке может быть записана как

$$P_m(t) = [\,p'(t)]^{m-1} \cdot p(t) = (\frac{\alpha \cdot t_0}{t_0 + t})^{m-1} \cdot [\frac{(1-\alpha)\cdot t_0 + t}{t_0 + t}]\,. \qquad (7)$$

На рис.1 представлены зависимости вероятностей взлома $P_m(t)$ от времени и от количества попыток взлома m. Из графиков видно, что с увеличением попыток взлома время на взлом уменьшается и, следовательно, при одном и том же уровне защищенности ТЗИ уменьшается вероятность взлома для одной попытки.

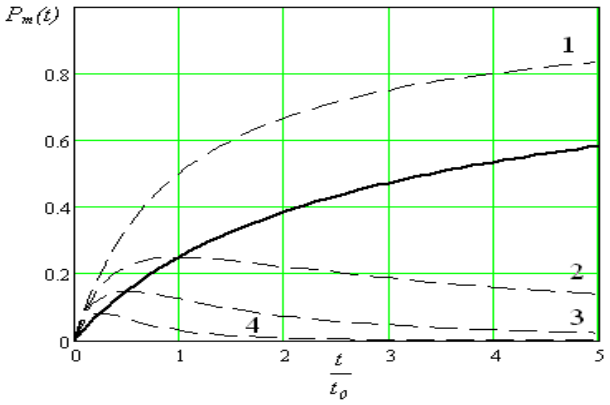

Рис.1. Зависимость вероятности взлома $P_m(t)$ от t/t_0 (приведенного времени) при $\alpha \approx 1$: кривая 1 соответствует взлому с одной попытки $m=1$, кривая 2 – с двух попыток $m=2$, кривая 3 - с трех попыток $m=3$, кривая 4 - после пяти попыток $m=5$. Сплошная линия соответствует $P(t)$ – максимумам вероятностей взлома

Определим кривую максимумов вероятностей взлома $P(t)$. Для этого определим вероятность m – той попытки взлома во времени. Для чего возьмем первую производную выражения (6) и приравняем ее нулю.

В результате вычислений получим зависимость попыток взлома от времени

$$m = \frac{t_0 + t}{(1-\alpha)\cdot t_0 + t}\,. \qquad (8)$$

Подстановка значения m во вторую производную указывает на максимум вероятности взлома при m –той попытке.

Подставив выражение (8) в (7), получим выражение для кривой максимумов вероятностей взлома ТЗИ от времени

$$P(t) = (\frac{\alpha \cdot t_0}{t_0 + t})^{\frac{\alpha \cdot t_0}{(1-\alpha)\cdot t_0 + t}} \cdot [\frac{(1-\alpha)\cdot t_0 + t}{t_0 + t}]\,. \qquad (9)$$

Эта зависимость $P(t)$ представлена на рис.1 сплошной линией.

Определим предельные значения вероятности взлома $P(t)$ при $t=0$ из выражения (9). При произвольных значениях α получим

$$P(t=0) = \alpha^{\frac{\alpha}{1-\alpha}} \cdot (1-\alpha)\,. \qquad (10)$$

При наличии защиты $\alpha \rightarrow 1$ вероятность взлома от времени будет равна

$$\lim_{\alpha \to 1} P(t=0) = 0 . \qquad (11)$$

Если $\alpha \to 0$, защита фактически отсутствует и вероятность взлома при этом от времени будет равна

$$\lim_{\alpha \to 0} P(t=0) = 1 . \qquad (12)$$

Определим предельные значения вероятности взлома $P(t)$ при $t \to \infty$ из выражения (9).

$$\lim_{t \to \infty} P(t=\infty) = \lim_{t=\infty} \left(\frac{\alpha \cdot t_0}{t_0 + t}\right)^{\frac{\alpha \cdot t_0}{(1-\alpha)\cdot t_0 + t}} \cdot \left[\frac{(1-\alpha)\cdot t_0 + t}{t_0 + t}\right] \approx \lim_{t \to \infty} \left(\frac{1}{t}\right)^{\frac{1}{t}} \left(\frac{t}{t}\right) = 1 . \qquad (13)$$

Из выражения (13) видно, что независимо от α предел вероятности взлома при $t \to \infty$ равен единице.

Таким образом, варьируя параметром α при t_0 и $t=0$ можно определить начальную вероятность взлома во времени, которую можно взять из статистических, экспериментальных или сертификационных данных ТЗИ, то есть при только что внедренной в работу ТЗИ.

Рассмотрим случай более эффективного использования ТЗИ. Это соответствует критерию $f(t_1) > f(0)$, то есть увеличению рисков защищенности. При этом условии, проделывая последовательно операции вычислений от (2) до (7), можно сделать заключение, что значения выражения (7) будут больше значений такого же вновь полученного выражения.

Чтобы отобразить этот факт и обеспечить требования вероятностей взлома с геометрическим распределением, можно представить полученное выражение в виде

$$P(t) = \left\{\left(\frac{\alpha \cdot t_0}{t_0 + t}\right)^{\frac{\alpha \cdot t_0}{(1-\alpha)\cdot t_0 + t}} \cdot \left[\frac{(1-\alpha)\cdot t_0 + t}{t_0 + t}\right]\right\}^{\gamma} , \qquad (14)$$

где γ – определяет критерий и является признаком эффективности использования ТЗИ во времени. Если $\gamma < 1$, то данная ТЗИ не обеспечит необходимой защиты во времени и такую защиту необходимо исключить из комплекса ТЗИ. Если $\gamma = 1$, то данная ТЗИ может быть применена, но ТЗИ обеспечивает минимальные требования по защите. При $\gamma > 1$ ТЗИ более эффективна в использовании и, чем γ больше единицы, тем эффективнее будет работать ТЗИ.

Определить γ можно из условий проведенной сертификации или статистических данных вероятностей взлома данной ТЗИ. Например, из данных сертификации имеем вероятность взлома $P(t_2)$ и t_2 – время, когда наступила эта вероятность взлома.

Чтобы определить γ подставим значения $P(t_2)$ и t_2 в (14) и возьмем логарифмы обеих частей уравнения. После преобразований получим

$$\gamma = \frac{lg\, P(t_2)}{lg\left\{\left(\frac{\alpha \cdot t_0}{t_0 + t_2}\right)^{\frac{\alpha \cdot t_0}{(1-\alpha)\cdot t_0 + t_2}} \cdot \left[\frac{(1-\alpha)\cdot t_0 + t_2}{t_0 + t_2}\right]\right\}} . \qquad (15)$$

Таким образом, если конкретно для данной ТЗИ известны экспериментальные, сертифицированные или статистические данные, то с помощью выражения (15) можно определить эффективность ее дальнейшего использования.

Для сравнения эффективности использования различных ТЗИ выражения (14) и (15) мало пригодны, так как значения t_0 для них могут не совпадать. Чтобы сравнивать разные

типы ТЗИ необходимо эти выражения привести к приведенному времени, то есть $t'=t/t_0$ и $t_2'=t_2/t_0$. В этом случае выражения (14) и (15) будет иметь вид

$$P(t') = \{(\frac{\alpha}{1+t'})^{\frac{\alpha}{(1-\alpha)+t'}} \cdot [\frac{(1-\alpha)+t'}{1+t'}]\}^{\gamma'} \quad (16)$$

и

$$\gamma' = \frac{lg\, P(t_2)}{lg\{(\frac{\alpha}{1+t'_2})^{\frac{\alpha}{(1-\alpha)+t'_2}} \cdot [\frac{(1-\alpha)+t'_2}{1+t'_2}]\}}. \quad (17)$$

Выводы. В результате проделанной работы можно сделать следующие выводы. Получено выражение и метод расчета вероятности взлома ТЗИ во времени. Выражение учитывает деградацию ТЗИ от момента создания до момента введения в эксплуатацию. В полученном выражении используется закон геометрического распределения вероятности взлома, что позволяет использовать теоретически полученные выражения для исследования защищенности информации во времени. Кроме того выражения учитывают и дают возможность рассчитывать и исследовать эффективность ТЗИ с использованием статистических, экспериментальных или сертификационных результатов или данных.

ЛИТЕРАТУРА

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных /Герасименко В.А. - В 2-х кн.: - М.: Энергоатомиздат. 1994, –576с.

2. Домарев В.В. Безопасность информационных технологий. Системный подход./ Домарев В.В. - К.: ООО ТИД ”ДС”, 2004. –992с.

3. Журиленко Б.Є. Оцінювання деградації стійкості комплексної системи захисту інформації в часі / Б.Є.Журиленко // Вісник НАУ: науковий журнал. – Київ, НАУ, 2007. - №1(31). - С.67-69.

4. Т.А.Голинкевич Оценка надежности радиоэлектронной аппаратуры. М.: Из-во «Советское радио». 1969. -176с.

5. Румшинский Л.З. Элементы теории вероятностей / Румшинский Л.З. - М.: Изд-во «Наука», Главн. Ред. Физ.-мат. Лит., 1970. 256 с.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Ігнатов В.О.