2. Кельтон В., Лоу А. Имитационное моделирование. Классика CS 3-е изд. – СПб.: Питер; Киев: Издательская группа BHV, 2004 – 847 с

УДК 681

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ) В МОБИЛЬНЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ (ИТКС)

Магистрант Коростелев В.К.
Канд. техн. наук, доцент Медведев Н.В.
МГТУ имени Н.Э. Баумана

Целью исследования является снижение рисков нарушения ИБ в ИТКС использующих технологию облачных вычислений при обработке информации различной степени конфиденциальности в операционных средах типа Android. Для решения проблемы предложен метод анализа данных на основе учета параметров уровня защищенности ресурсов облачной ИТКС.

Использование Байесовского подхода для анализа потенциальных угроз ИТКС, основанных на использовании операционных сред типа Android, даст возможность осуществить выявление зависимости между факторами влияющими на ИБ;

В случае анализа уровня защищенности ресурсов ИТКС рассматривается случайная величина Y, которая имеет плотность вероятности с параметрами δ. На основании полученных статистических данных можно сделать вывод о другой случайной величине δ, имеющей распределение вероятности $\pi(\delta)$. Тогда согласно формуле Байеса

$$p(\delta \mid y) = \frac{p(y \mid \delta)P(\delta)}{p(y)}$$

Основными признаками защищенности ресурсов облачной ИТКС служит следующий кортеж показателей: способность обеспечить конфиденциальность (C), целостность (N) и доступность (M) информации при воздействии угроз определенного типа.

Если одновременно получены три показателя, то в соответствии с теоремой Байеса, используется формула

$$P(\delta_i/C,N,M) = \frac{P(C/\delta_i)P(N/\delta_i)P(M/\delta_i)P(\delta_i)}{\sum_{i=1}^{3} P(C/\delta_i)P(N/\delta_i)P(M/\delta_i)P(\delta_i)}$$

Если в результате исследования выяснилось, что СЗИ не обеспечила кортеж показателей защищенности информации при воздействии угрозы, то необходимо рассматривать противоположные события:

$$P(\overline{CNM}/\delta_i) = 1 - P(C,N,M/\delta_i).$$

Литература

1. Оценка информационной безопасности телекоммуникационных систем: Учебное пособие». - В.Г. Кулаков, А.Б. Андреев, А.В. Заряев и др.— Воронеж: Воронежский институт МВД России, 2013. — 305 с.

2. Jeff Six, «Application Security For The Android Platform», O'Reilly Media, 2011.

УДК 681

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (НСД) К ИНФОРМАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ (АС)

Аспирант Ковынёв Н.В.
Канд. техн. наук, доцент Медведев Н.В.
МГТУ имени Н.Э. Баумана

Показатели эффективности тех или иных методов защиты лучше всего выражать вероятностной мерой, так как учитываются факторы, имеющие чисто случайный характер. Все исходы событий НСД любых атак будут представлять собой группу несовместных событий, сумма вероятностей которых, исходя из теории вероятностей, будет равна единице. В таком случае, сумма вероятностей событий фильтрации НСД есть вероятность обеспечения безопасности информации при применении средства фильтрации. Всего есть X, которые и будут обозначать предотвращение попыток НСД.

$$\sum_{i=\mathrm{I}}^{\mathrm{X}} P_i = 1,$$

где P_i – вероятность *i*-го итогового события.

В этом случае можно определить вероятность нахождения системы в защищенном состоянии:

$$P_{\mathrm{I}} = p_1(a_1, \dots, a_n);$$
$$P_{\mathrm{i}} = p_i(a_1, \dots, a_n);$$
$$P_{\mathrm{x}} = p_x(a_1, \dots, a_n);$$

Исходя из приведенных выше данных, вероятность преодоления средства фильтрации, то есть получения НСД к информационно-вычислительным ресурсам распределенной АС, можно определить как:

$$P_{\text{НСД}} = 1 - \sum_{i=I}^{V} P_i = = 1 - p_1(a_1, \dots, a_n)) - \dots p_i(a_1, \dots, a_n)) - \cdots p_n(a_1, \dots, a_n)),$$

Таким образом, судить об эффективности средства фильтрации можно по значению $\mathrm{P_{НСД}}$. Введем функцию $\mathrm{F(P_{НСД})}$ и будем считать, что средство