ИНФОРМАЦИЯ И БЕЗОПАСНОСТЬ. 2012. №1. с.89-92

УДК 681.3:519.1

ОСОБЕННОСТИ РЕАЛИЗАЦИИ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ОЦЕНКИ ХАРАКТЕРИСТИК УГРОЗ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

С.В. Скрыль, В.К. Джоган, В.В. Киселев, А.В. Демченков

Рассматривается комплекс математических моделей для оценки характеристик угроз безопасности использования информационных технологий. Приводится выражение для определения значений интегральной характеристики такого рода угроз

Ключевые слова: математические модели, угрозы безопасности использования информационных технологий

С учетом классификационных оснований /1/, систематизирующих характеристики угроз безопасности использования информационных технологий /2/ и требования однородности этих характеристик в качестве оценочного параметра множества первичных характеристик этих угроз условимся использовать интенсивность $\lambda_i^{(1)}$ их проявления.

Вместе с тем, случайный характер воздействия угроз приводит к необходимости рассматривать интенсивность их проявления как случайную характеристику. С учетом данного обстоятельства вся система характеристик угроз безопасности использования информационных технологий оценивается как вероятностная, что позволяет представить вторичные характеристики угроз как случайные события, вызванные проявлением их первичных характеристик. Аналогичным образом обобщенные характеристики представляются как случайные события, вызванные проявлением вторичных характеристик, а интегральная характеристика представляется как случайное событие, вызванное проявлением обобщенных характеристик.

С учетом изложенного при формировании вторичных характеристик условимся использовать вероятность проявления соответствующих угроз.

Для множества, вторичных характеристик определим условие проявления угрозы в виде неравенства:

$$\lambda_j^{(2)} > r_j^{(2)}, \qquad (1)$$

в котором $\lambda_j^{(2)}$ – интенсивность проявления угрозы, $r_j^{(2)}$ – ее пороговое значение, обусловленное работой средств обеспечения безопасности использования информационных технологий.

Величины $\lambda_j^{(2)}$ и $r_j^{(2)}$, входящие в условие (1) являются случайными величинами. Среднее значение вероятности выполнения этого условия является значением j-й вторичной характеристики угроз безопасности использования информационной технологий:

$$p_j^{(2)} = P\left(\lambda_j^{(2)} > r_j^{(2)}\right). \qquad (2)$$

При определении значений (2) воспользуемся представлением работы средств защиты информации с позиций классической теории обеспечения безопасности использования информационных технологий /3/. Это позволяет случайную величину $r_j^{(2)}$ интенсивности проявления угрозы, при которой средства защиты обеспечивают требуемый уровень безопасности использования информационных технологий, с достаточной степенью достоверности аппроксимировать экспоненциальным законом распределения. Это, в свою очередь, позволяет для определения (2) использовать выражение:

$$\overline{p}_j^{(2)} = 1 - \exp\left(-\frac{\overline{\lambda}_j^{(2)} - r_{j(\min)}^{(2)}}{\overline{r}_j^{(2)}}\right), \qquad (3)$$

Скрыль Сергей Васильевич - МГТУ им. Н.Э. Баумана, профессор кафедры «Защита информации», д-р техн. наук, профессор тел. (495) 632-22-47

Джоган Василий Климович - МГТУ им. Н.Э. Баумана, канд. техн. наук, соискатель, тел. (495) 632-22-47

Киселев Вадим Вячеславович - ВИ МВД РФ, канд. техн. наук, старший преподаватель, e-mail: moriarty@bk.ru

Демченков Александр Владимирович – ВГТУ, аспирант, e-mail: aleandr.rdo.201@gmail.com

в котором $\overline{\lambda}_j^{(2)}$ и $\overline{r}_j^{(2)}$ – средние значения случайных величин $\lambda_j^{(2)}$ и $r_j^{(2)}$, соответственно, а $r_{j(\min)}^{(2)}$ – минимальное значение величины $r_j^{(2)}$.

При определении значений $\overline{\lambda}_j^{(2)}$ воспользуемся композиционными причинно-следственными связями между классами угроз безопасности использования информационных технологий /1/.

Ниже приводятся выражения для формирования аналитических моделей, позволяющие определять значения интенсивности $\overline{\lambda}_j^{(2)}$, j = 1, 2, …, 11, проявления угроз, классифицируемых в /1/ как вторичные. Основу этих моделей составляют разработанные в /3/ методы.

1) среднее значение интенсивности проявления угрозы независимо от активности объекта информатизации (ОИ):

$$\overline{\lambda}_1^{(2)} = M\left(\lambda_1^{(1)} \circ \lambda_5^{(1)} \circ \lambda_{12}^{(1)}\right) =$$

$$= \int_0^{\infty}\int_0^{q}\int_0^{q_{II}} q \cdot f_1^{(1)}(q_I)\cdot f_5^{(1)}(q_{II}-q_I)\cdot f_{12}^{(1)}(q-q_{II})\,dq_I\,dq_{II}\,dq,$$

где $f_1^{(1)}$, $f_5^{(1)}$ и $f_{12}^{(1)}$ – плотности распределения вероятностей случайных величин:

$\lambda_1^{(1)}$ – интенсивности проявления угрозы, естественного характера;

$\lambda_5^{(1)}$ – интенсивности проявления угрозы, непосредственным источником которой является природная среда;

$\lambda_{12}^{(1)}$ – интенсивности проявления угрозы, источник которой в ОИ заложен конструктивно;

$M(*)$ – математическое ожидание величины *;

$\circ$ – знак операции композиции случайных величин.

2) среднее значение интенсивности проявления угрозы, которая при реализации ничего не меняет в структуре и содержании информации ОИ:

$$\overline{\lambda}_2^{(2)} = M\left(\lambda_9^{(1)} \circ \lambda_{10}^{(1)}\right) = \int_0^{\infty} q \int_0^{\infty} f_9^{(1)}(q-q_I)\cdot f_{10}^{(1)}(q_I)\,dq_I\,dq,$$

где $f_9^{(1)}$ и $f_{10}^{(1)}$ - плотности распределения вероятностей случайных величин:

$\lambda_9^{(1)}$ – интенсивности проявления угрозы, источник которой расположен вне контролируемой зоны территории (помещения), на которой находятся элементы ОИ;

$\lambda_{10}^{(1)}$ – интенсивности проявления угрозы, источник которой расположен в пределах контролируемой зоны территории (помещения), на которой находятся элементы ОИ.

3) среднее значение интенсивности проявления угрозы, которая при воздействии вносит изменения в структуру и содержание информации ОИ:

$$\overline{\lambda}_3^{(2)} = M\left(\lambda_7^{(1)} \circ \lambda_8^{(1)}\right) = \int_0^{\infty} q \int_0^{\infty} f_7^{(1)}(q-q_I)\cdot f_8^{(1)}(q_I)\,dq_I\,dq,$$

где $f_7^{(1)}$ и $f_8^{(1)}$ – плотности распределения вероятностей случайных величин:

$\lambda_7^{(1)}$ - интенсивности проявления угрозы, непосредственным источником которой является работа санкционированных программно-аппаратных средств;

$\lambda_8^{(1)}$ - интенсивности проявления угрозы, непосредственным источником которой является работа несанкционированных программно-аппаратных средств.

4) среднее значение интенсивности проявления угрозы на этапе доступа к информационным ресурсам ОИ:

$$\overline{\lambda}_4^{(2)} = M\left(\lambda_6^{(1)} \circ \lambda_{11}^{(1)}\right) = \int_0^{\infty} q \int_0^{\infty} f_6^{(1)}(q-q_I)\cdot f_{11}^{(1)}(q_I)\,dq_I\,dq,$$

где $f_6^{(1)}$ и $f_{11}^{(1)}$ – плотности распределения вероятностей случайных величин:

$\lambda_6^{(1)}$ – интенсивности проявления угрозы, непосредственным источником которой является человек;

$\lambda_{11}^{(1)}$ – интенсивности проявления угрозы, источник которой имеет доступ к периферийным устройствам (терминалам) ОИ.

5) среднее значение интенсивности проявления угрозы после разрешения доступа к информационным ресурсам ОИ:

$$\overline{\lambda}_5^{(2)} = M\left(\lambda_3^{(1)} \circ \lambda_6^{(1)}\right) = \int_0^{\infty} q \int_0^{\infty} f_3^{(1)}(q - q_{\text{I}}) \cdot f_6^{(1)}(q_{\text{I}}) dq_{\text{I}}\, dq,$$

где $f_3^{(1)}$ – плотность распределения вероятности случайной величины $\lambda_3^{(1)}$ – интенсивности проявления угрозы случайного характера.

6) среднее значение интенсивности проявления угрозы, направленной на использование прямого стандартного пути доступа к информационным ресурсам ОИ:

$$\overline{\lambda}_6^{(2)} = M\left(\lambda_4^{(1)} \circ \lambda_6^{(1)}\right) = \int_0^{\infty} q \int_0^{\infty} f_4^{(1)}(q - q_{\text{I}}) \cdot f_6^{(1)}(q_{\text{I}}) dq_{\text{I}}\, dq,$$

где $f_4^{(1)}$ – плотность распределения вероятности случайной величины $\lambda_4^{(1)}$ – интенсивности проявления угрозы преднамеренного характера.

7) среднее значение интенсивности проявления угрозы, направленной на использование скрытого нестандартного пути доступа к информационным ресурсам ОИ:

$$\overline{\lambda}_7^{(2)} = M\left(\lambda_3^{(1)} \circ \lambda_4^{(1)}\right) = \int_0^{\infty} q \int_0^{\infty} f_3^{(1)}(q - q_{\text{I}}) \cdot f_4^{(1)}(q_{\text{I}}) dq_{\text{I}}\, dq.$$

8) среднее значение интенсивности проявления угрозы доступа к информации на внешних запоминающих устройствах:

$$\overline{\lambda}_8^{(2)} = M\left(\lambda_2^{(1)} \circ \lambda_4^{(1)} \circ \lambda_6^{(1)} \circ \lambda_{11}^{(1)}\right) =$$

$$= \int_0^{\infty}\int_0^{q}\int_0^{q_1}\int_0^{q_3} q \cdot f_2^{(1)}(q_1) \cdot f_4^{(1)}(q_2 - q_1) \cdot f_6^{(1)}(q_3 - q_2) \cdot$$

$$\cdot f_{11}^{(1)}(q - q_3) dq_1\, dq_2 dq_3 dq,$$

где $f_2^{(1)}$ – плотность распределения вероятности случайной величины $\lambda_2^{(1)}$ – интенсивности проявления угрозы искусственного характера.

9) среднее значение интенсивности проявления угрозы доступа к информации в оперативной памяти:

$$\overline{\lambda}_9^{(2)} = M\left(\lambda_2^{(1)} \circ \lambda_4^{(1)} \circ \lambda_{11}^{(1)}\right) =$$

$$= \int_0^{\infty}\int_0^{q}\int_0^{q_{\text{II}}} q \cdot f_2^{(1)}(q_{\text{I}}) \cdot f_4^{(1)}(q_{\text{II}} - q_{\text{I}}) \cdot f_{11}^{(1)}(q - q_{\text{II}}) dq_{\text{I}}\, dq_{\text{II}} dq.$$

10) среднее значение интенсивности проявления угрозы доступа к информации в оперативной памяти:

$$\overline{\lambda}_{10}^{(2)} = M\left(\lambda_3^{(1)} \circ \lambda_4^{(1)} \circ \lambda_9^{(1)}\right) =$$

$$= \int_0^{\infty}\int_0^{q}\int_0^{q_{\text{II}}} q \cdot f_3^{(1)}(q_{\text{I}}) \cdot f_4^{(1)}(q_{\text{II}} - q_{\text{I}}) \cdot f_9^{(1)}(q - q_{\text{II}}) dq_{\text{I}}\, dq_{\text{II}} dq.$$

11) среднее значение интенсивности проявления угрозы доступа к информации, циркулирующей в линиях связи:

$$\overline{\lambda}_{11}^{(2)} = M\left(\lambda_3^{(1)} \circ \lambda_4^{(1)} \circ \lambda_{11}^{(1)}\right) =$$

$$= \int_0^{\infty}\int_0^{q}\int_0^{q_{\text{II}}} q \cdot f_3^{(1)}(q_{\text{I}}) \cdot f_4^{(1)}(q_{\text{II}} - q_{\text{I}}) \cdot f_{11}^{(1)}(q - q_{\text{II}}) dq_{\text{I}}\, dq_{\text{II}} dq.$$

При формировании выражений для определения значений обобщенных характеристик воспользуемся композиционными причинно-следственными связями между классами угроз безопасности использования информационных технологий /1/. Ниже приводятся выражения для определения значений множества обобщенных характеристик, первое, третье и пятое из которых соответствуют положениям центральной предельной теоремы теории вероятностей /4/, а второе и четвертое - разработанным в /3/ аналитическим моделям:

$$y_1^{(3)} = \frac{1}{5}\left(\overline{p}_1^{(2)} + \overline{p}_2^{(2)} + \overline{p}_5^{(2)} + \overline{p}_6^{(2)} + \overline{p}_7^{(2)}\right);$$

$$y_2^{(3)} = \frac{1}{4} M\left(y_3^{(2)} \circ y_5^{(2)} \circ y_6^{(2)} \circ y_7^{(2)}\right) =$$

$$= \frac{1}{4}\int_0^{\infty}\int_0^{q}\int_0^{q_1}\int_0^{q_3} q \cdot f_3^{(2)}(q_1) \cdot f_5^{(2)}(q_2 - q_1) \cdot f_6^{(2)}(q_3 - q_2) \cdot$$

$$\cdot f_7^{(2)}(q - q_3) dq_1\, dq_2 dq_3 dq,$$

где $f_3^{(2)}$, $f_5^{(2)}$, $f_6^{(2)}$ и $f_7^{(2)}$ – плотности распределения вероятностей случайных величин $p_3^{(2)}$, $p_5^{(2)}$, $p_6^{(2)}$ и $p_7^{(2)}$, соответственно;

$$y_3^{(3)} = \frac{1}{9}(\overline{p}_3^{(2)} + \overline{p}_4^{(2)} + \overline{p}_5^{(2)} + \overline{p}_6^{(2)} +$$

$$+ \overline{p}_7^{(2)} + \overline{p}_8^{(2)} + \overline{p}_9^{(2)} + \overline{p}_{10}^{(2)} + \overline{p}_{11}^{(2)});$$

$$y_4^{(3)} = \frac{1}{3} M\left(y_3^{(2)} \circ y_5^{(2)} \circ y_7^{(2)}\right) =$$

$$= \frac{1}{3}\int_0^{\infty}\int_0^{q}\int_0^{q_{\text{II}}} q \cdot f_3^{(2)}(q_{\text{I}}) \cdot f_5^{(2)}(q_{\text{II}} - q_{\text{I}}) \cdot$$

$$\cdot f_7^{(2)}(q - q_{\text{II}}) dq_{\text{I}}\, dq_{\text{II}} dq,$$

где $f_3^{(2)}$, $f_5^{(2)}$, и $f_7^{(2)}$ – плотности распределения вероятностей случайных величин $y_3^{(2)}$, $y_5^{(2)}$ и $y_7^{(2)}$, соответственно;

$$y_5^{(3)} = \frac{1}{6}\left(\overline{p}_3^{(2)} + \overline{p}_4^{(2)} + \overline{p}_5^{(2)} + \overline{p}_6^{(2)} + \overline{p}_7^{(2)} + \overline{p}_{10}^{(2)}\right).$$

С целью аналитического представления интегральной характеристики угроз безопасности использования информацион-ных технологий рассмотрим вероятностную интерпретацию группы событий, связанных с проявлением обобщенных характеристик угроз.

Для этого определим следующие события: событие 1 – «Воздействие угроз безопасности использования информационных технологий». Его составляют пять событий: событие 2 – «Проявление угрозы нарушения конфиденциальности информации ОИ», событие 3 – «Проявление угрозы нарушения целостности информации ОИ», событие 4 – «Проявление угрозы нарушения доступности информации ОИ», событие 5 – «Проявление угрозы перехвата информации о структуре, разрешенных сервисах, способах их реализации и существующих уязвимостях элементов ОИ» и событие 6 – «Проявление угрозы блокировки межсетевого взаимодействия внутри ОИ либо между ОИ».

События 2 ÷ 6 составляют полную группу событий, причем события 2 и 5, 3 и 6 являются попарно взаимозависимыми.

Запишем выражение, связывающее вероятности рассмотренных событий:

$$P_{(y)} = 1 - (1 - y_2^{(3)}) \cdot (1 - y_1^{(3)} \cdot y_4^{(3)}) \cdot (1 - y_3^{(3)} \cdot y_5^{(3)}).$$

Полученное с помощью рассмотренных моделей выражение для определения значений интегральной характеристики угроз безопасности использования информационных технологий может быть использовано для оценки защищенности информационных процессов на объектах информатизации различного назначения.

Литература

1. Классификационные основания для систематизации угроз информационной безопасности информационной сферы / В.В. Киселев, Т.В. Мещерякова, Д.В. Юдин, В.С. Середа // Информация и безопасность. – Воронеж: ВГТУ, 2011. Вып. 3. – С. 451 – 454.

2. Теоретические основы компьютерной безопасности: учеб пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков [и др.]. - М.: Радио и связь, 2000. - 192 с.

3. Оценка защищенности информационных процессов в территориальных ОВД: модели исследования: монография / под ред. С.В. Скрыля. – Воронеж: Воронежский институт МВД России, 2009. – 217 с.

4.Вентцель Е.С. Теория вероятностей: учебник / Е.С. Вентцель – 11-е изд. – М.: КНОРУС, 2010. – 664 с.

Московский государственный технический университет имени Н.Э. Баумана
The Moscow state technical university of a name of N.E. Bauman

FEATURES OF REALIZATION OF MATHEMATICAL MODELS FOR THE ESTIMATION OF CHARACTERISTICS OF THREATS OF SAFETY OF USE INFORMATION TECHNOLOGIES

S.V. Skryl, V.K. Dzhogan, V.V. Kiselev, A.V. Demchenkov

The complex of mathematical models for an estimation of characteristics of threats of safety of use of information technologies is considered. Expression for definition of values of the integrated characteristic of such threats is resulted

Key words: mathematical models, threats of safety of use of information technologies