УДК 002:004.056 + 001.891.573 + 004.056

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Ф. Абраменков, А.И. Баландин, В.Ю. Бердюгин

В данной статье рассмотрена проблема выбора метода математического моделирования угроз информационной безопасности. На основе наиболее часто встречающихся проблем информационной безопасности представлены четыре основных метода моделирования. Представлены основные положения каждой модели. Определены критерии сравнения данных методов. Представлен наиболее удачный, по мнению авторов статьи, вариант решения проблемы защиты информационных систем, выбранный на основе сравнительного анализа всех четырех методов, опирающегося на выделенные критерии.

Ключевые слова: информация, безопасность, математическая модель, угроза безопасности, злоумышленник, автоматизированная информационная система, защита информации.

В настоящее время информатика становится не только лидирующим, но и доминирующим направлением современного научно-технологического прогресса, основным фронтом развернувшейся в мире борьбы за научно-техническое и экономическое превосходство. Данное соперничество все чаще приобретает форму активной борьбы, называемой информационной борьбой, стали появляться угрозы информационной безопасности. Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Целью информационной борьбы является обеспечение необходимой степени собственной информационной безопасности и снижение уровня информационной безопасности противостоящий стороны до значения, не обеспечивающее его существования и развития. Информационная безопасность – состояние сохранности информационных ресурсов и защищённости законных прав личности и общества в информационной сфере. Для изучения задачи защиты информации необходимо построить математическую модель. Математическая модель – математическое представление реальности, один из вариантов модели, как системы, исследование которой позволяет получать информацию о некоторой другой системе [1].

Применение математического моделирования подразумевает замену реального объекта его математической моделью. Это необходимо для того, чтобы наиболее полно и тщательно рассмотреть исследуемый вопрос, минимизировать материальные затраты, а также уменьшить срок исследования проблемы для ее последующего решения, ведь с появлением ЭВМ стало возможным вычислять огромное количество операций за короткий срок.

Обращаясь к проблеме информационной безопасности, стоит отметить, что это относительно новая ветвь технической науки, которая нуждается в модернизации, учитывая стремительные темпы прогресса информационных технологий. Таким образом, данная проблема является актуальной.

Мы взяли наиболее часто встречающиеся проблемы ИБ и на их основе составили математические модели. В итоге мы сформировали 3 модели, каждая из которых имела те или иные преимущества над другими:

1. Математическое моделирование при помощи блок-схем.
2. Математическая модель угроз безопасности информационных ресурсов.
3. Общая математическая модель.

В качестве критериев мы брали такие факторы, как эффективность, универсальность и применение на практике, что позволило выделить одну наиболее привлекательную модель.

1. Математическое моделирование при помощи блок-схем [2]

Предположим, что автоматизированная информационная система (АИС) может находиться в n-возможных случайных состояниях $x_1, x_2, \ldots, x_n$. Состояние перехода АИС из i-го в j-е состояние тоже является случайным и характеризуется вероятностью P_{ij}. Если для каждого состояния известны вероятности перехода АИС в любое другое состояние, то можно составить матрицу переходных вероятностей вида:

$$\left\|P_{ij}\right\| = \begin{vmatrix} P_{11} & P_{12} & \ldots & P_{1j} & \ldots & P_{1n} \\ P_{21} & P_{22} & \ldots & P_{2j} & \ldots & P_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ P_{i1} & P_{i2} & \ldots & P_{ij} & \ldots & P_{in} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ P_{n1} & P_{n2} & \ldots & P_{nj} & \ldots & P_{nn} \end{vmatrix}. \qquad (1)$$

Пусть в начальный момент АИС находится в состоянии x_n. Тогда, для начального момента (n=0) вероятности всех состояний равны нулю, кроме вероятности начального состояния $P_n(0)=1$. После первого шага $(k=1)$ АИС с учетом (1) перейдет из состояния x_n в одно из состояний $x_1, x_2, \ldots, x_n, \ldots, x_k$ с вероятностями; $P_{n1}, P_{n2}, \ldots, P_{nn}, \ldots, P_{nk}$. Тогда n-я строчка матрицы переходных вероятностей будет иметь вид:

$$P_1(1) = P_{n1};\ P_2(1) = P_{n2} \ldots,\ P_n(1) = P_{nn},\ \ldots,\ P_k(1) = P(nk) \qquad (2)$$

Вероятности состояний после второго шага определяются по формуле полной вероятности. Тогда:

$$P_i(2)=\sum_{i=1}^{3} P_j(1)\cdot P_{ij} \cdot \qquad (3)$$

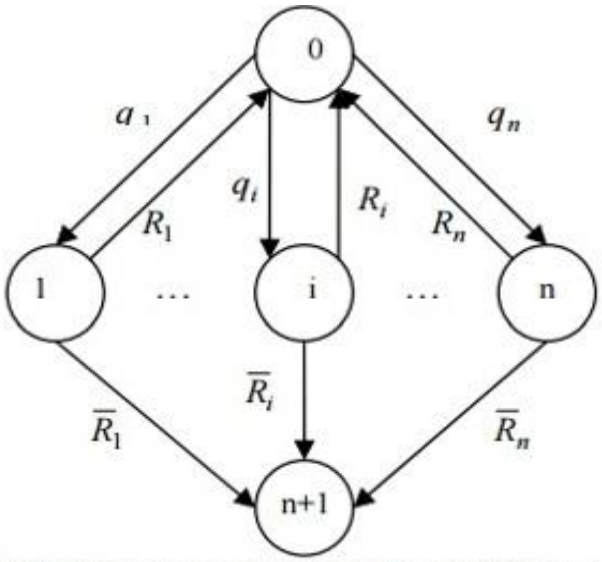
При этом должна выполняться гипотеза о том, что АИС после первого шага может быть в любом из возможных состояний. Тогда с учетом (2) и в соответствии с (3) по формуле полной вероятности матрица переходных вероятностей после k-го шага будет иметь вид:

$$P_i(k)=\sum_{j=1}^{k} P_j(k-1)P_{ji} \cdot$$

где $i=1,2,\ldots,k;$

Примем следующие обозначения: R_i и $\overline{Ri} = 1\text{-}R_i$ – вероятности соответственно успешного и неуспешного парирования возникшей i-й внутренней угрозы; q_i и $P_i=1\text{-}q_i$ – вероятности соответственно возникновения и не возникновения i-й внутренней угрозы; $0,1,\ldots,i,\ldots,n,n+1$ – состояния, в которых может оказаться рассматриваемая система в результате воздействия n независимых внутренних угроз. При этом, состояние $n+1$ соответствует поглощающему состоянию.

Для указанного выше случая граф состояний представлен на рис.



Граф состояния системы при воздействии на нее n независимых внутренних угроз

Как видно из рис., при любом i-м воздействии система может оказаться с вероятностью R_i в исходном состоянии, что соответствует успешному отражению i-й внутренней угрозы, и с вероятностью $\bar{R}_i=1\text{-}R_i$ в поглощающем состоянии $n+1$, что соответствует реализации злоумышленником i-й внутренней угрозы.

В соответствии с рис. матрица переходных вероятностей будет иметь следующий вид:

$$\|P_{ij}\| = \begin{vmatrix} q_{00} & q_1 & \dots & q_i & \dots & q_n & 0 \\ R_1 & q_{11} & \dots & 0 & \dots & 0 & \overline{R}_1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ R_n & 0 & \dots & 0 & \dots & q_{nn} & \overline{R}_n \\ 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{vmatrix},$$

где $q_{00} = 1-q_{\sum}$

Определим вероятность перехода системы в любое *i*-е состояние для следующих исходных данных: $P_0(0)=1$ и $P_1(0)=\dots=P_i(0)=\dots=P_n(0)=P_{n+1}(0)=0$.

Исходя из всего вышесказанного, данная модель обладает возможностью применения на практике, довольно высокой эффективностью и универсальностью. Сильной стороной этой модели является её наглядность. Действительно, использование блок-схем позволяет упростить процесс обучения данному способу обеспечения информационной безопасности.

2. Математическая модель угроз безопасности информационных ресурсов [3]

Пусть $A \in A_1*A_2*\dots*A_8$ – множество моделей атак, где A_i $(i=\overline{1,9})$ – множество значений *i*-го параметра модели атаки, определяющего тип атаки. Каждая модель $\vec{a}_i \in A_i$.

Модель злоумышленника задается в виде вектора $\vec{b} \in B$, где $B \in B_1*B_2*\dots*B_6$, B_j $(j=\overline{1,6})$ – множество значений *j*-го параметра модели злоумышленника, а модель АИС – $\vec{c} \in C$, где $C \in C_1*C_2*\dots*C_6$, C_k $(k=\overline{1,6})$ – множество значений *k*-го параметра модели АИС.

С каждой атакой будем связывать значение риска, вычисляемое по общеизвестной формуле на основе двух факторов – вероятности происшествия и тяжести возможных последствий: *Риск = Влияние*Вероятность.*

Обозначим через $R: A*B*C\rightarrow[0;1]$ функцию, задающую уровень риска, связанного с атакой $\vec{a} \in A$ в условиях, когда она может быть применена злоумышленником $\vec{b} \in B$ для взлома АИС $\vec{c} \in C$.

Пусть $I: C*A\rightarrow[0;1]$ – функция влияния. Под влиянием понимается степень ущерба от применения атаки $\vec{a} \in A$ к АИС $\vec{c} \in C$.

Пусть $P: B*A\rightarrow[0,1]$ – вероятность того, что злоумышленник $\vec{b} \in B$ предпримет атаку $\vec{a} \in A$, т.е. обладает ресурсами для ее осуществления и сочтет эту атаку целесообразной.

Тогда функция риска *R* выражаются следующим образом:

$$R(\vec{a},\vec{b},\vec{c}) = I(\vec{c},\vec{a})*P(\vec{b},\vec{a}).$$

Определим функцию $I(\vec{c},\vec{a})$. Для этого рассмотрим семейство функций I_{gh}: $C_g * A_h \to R_+$... где R_+ – множество неотрицательных действительных чисел. Здесь функция I_{gh} задает уровень взаимного влияния параметра ИАС C_g и параметра атаки a_h:

- $I_{gh}(c,a)=0$, если атака со значением параметра $a \in A_h$ не применима к АИС со значением параметра $c \in C_g$;
- $0 < I_{gh}(c,a) < 1$, если значение параметра ИАС $c \in C_g$ снижает вероятность успешного применения атаки со значением параметра $a \in A_h$;
- $I_{gh}(c,a) = 1$,если значение параметра АИС $c \in C_g$ не влияет на применимость атаки с параметром $a \in A_h$;
- $I_{gh}(c,a) > 1$, если значение параметра АИС $c \in C_g$ указывает на то, что атака с параметром $a \in A_h$ применима для ее взлома.

Обозначим через $I_{gh} : C_g * A_h \to [0; 1]$ нормированную функцию:

$$\overline{I_{gh}}(c,a) = \frac{I_{gh}(c,a)}{\sum_{\xi \in C_g} I_{gh}(\xi,a)}.$$

Тогда уровень ущерба от применения атаки $\bar{a} \in A$ к АИС $\bar{c} \in C$ вычисляется по следующей формуле:

$$I(\vec{c},\vec{a}) = \min_{h=\overline{1,9}} \prod_{g=1,5} \overline{I_{gh}}(c_g,a_h),$$

где атака и АИС заданы параметрами $(a_1, a_2, ..., a_9)$ и $(c_1, c_2, ..., c_6)$ соответственно. Заметим, что уровень влияния всех параметров АИС на применимость атаки с заданным значением параметра в этой формуле вычисляется по мультипликативному критерию: $\prod_{g=1}^{6} \overline{I_{gh}}(c_g,a_h)$. Если значение хотя бы одного из параметров АИС противоречит возможности применения атаки, то результатом оценки применимости атаки к АИС будет нулевое значение, что соответствует нулевому уровню ущерба от атаки.

Функция $P(\vec{b},\vec{a})$, определяющая зависимость между параметрами $(a_1, a_2, ..., a_9)$ атаки и $(b_1, b_2, ..., b_6)$ злоумышленника, выражается аналогично функции $I(\vec{c},\vec{a})$.

Таким образом, общая формула для определения уровня риска, связанного с атакой $\vec{a} \in A$ в условиях, когда эта атака может быть применена злоумышленником $\vec{b} \in B$ для взлома АИС $\vec{c} \in C$, имеет вид:

$$\Re(\vec{a},\vec{b},\vec{c}) = \min_{h=\overline{1,9}} \prod_{g=\overline{1,6}} \overline{I_{gh}}(c_g,a_h) * \min_{h=\overline{1,9}} \prod_{t=\overline{1,6}} \overline{P_{th}}(b_t,a_h).$$

Будем считать, что АИС $\vec{c} \in C$ подвержена атаке $\vec{a} \in A$ в условиях, когда ей угрожает злоумышленник $\vec{b} \in B$, если $R(\vec{a}, \vec{b}, \vec{c}) > 0$.

Данный метод может оказаться весьма полезным на любом предприятии, обладая при этом довольно высоким показателями эффективности. Универсальность модели оставляет желать лучшего.

3. Общая математическая модель [4]

Математическое представление модели включает семь абстрактных пространств *K, V, L, A, C, H* и *Ψ*, источники угроз *к, j, v, l, c, h, ψ*, априорные вероятности источников угроз *π(k), P (jk/k), P (к/jk),* условные вероятности *P (jk/l), P (к/l), P (K/L),* и решающую функцию *D (a/K, C)*.Таким образом, источник угрозы *k* может быть реализован различными способами *jk*. За вероятность существования источника угрозы (область *k*) отвечает априорная вероятность *π (к)*. За вероятность реализации *jk* отвечает условная вероятность *P (jk/k)*. Тогда вероятность совместного распределения угрозы *k* и способов ее реализации *jk* будет определяться зависимостью:

$$P(k, jk) = \pi(k)\, P(jk/k). \quad (1)$$

Выражение (1) совместно с пространством К будет составлять математическое описание оценки источников угроз.

Таким образом, мы имеем источники угроз (*k*), способы их реализации (*jk*) в пространстве. И всё это (в пространстве *K*) управляется функцией плотности вероятности *P (k, jk)*. Она определяет вероятность существования источников угроз и их характеристики, вероятность реализации конкретного способа их воздействия на объект защиты.

Пространство информационных объектов *L* представляет собой множество точек *l* по одной на каждый объект

$$\{l\} \subset L.$$

Отображение точек пространства *K* в точки пространства *L*, т.е. воздействие источников угроз *k*, а точнее, реализация конкретных способов воздействия *jk* источников угроз *k* на объекты *l* информационной среды, описываются вероятностным законом. Определим его условной вероятностью:

P (jk/l) – условная вероятность воздействия способа реализации *jk* угрозы *k* на объект защиты *l*: *P (jk/l): jk→ l,*

P (к/l) – условная вероятность воздействия угрозы *k* всеми способами *jk* на объект защиты *l: P (k/l): k →l,* (4)

P (K/L) – условная вероятность воздействия всех угроз *K* на все объекты защиты *L: P (K/L): K→ L.*

Пространство важности информационных объектов *V* образовано множеством точек V_l, каждая из которых отображает важность соответствующего информационного объекта *l*. Под понятием «важность» понимается оценка принесённого ущерба после реализации способа воздействия *jk*

дестабилизирующего фактора k на объект l. Отображение точек l пространства L в точки V_l пространства V осуществляется по аналитическим или экспертным оценкам: $l \rightarrow V_l | jk \rightarrow l,\ k \rightarrow l,\ K \rightarrow L$ (5).

Пространство средств защиты C включает в себя множество точек $c_{i,\,jk,\,k,\,l}$:

$$\{c_{i,\,jk,\,k,\,l}\} \subset C$$

При этом точкам $c_{i,\,jk,\,k,\,l}$ соответствует i-е средство по противодействию jk-му способу реализации k-й угрозы объекту защиты l.

Пространство оценок эффективности средств защиты H представляет собой совокупность точек h.

Здесь под точкой $h_{i,\,jk,\,k,\,l}$ понимается значение эффективности средства противодействия $c_{i,\,jk,\,k,\,l}$, которое показывает степень эффективности выполнения $c_{i,\,jk,\,k,\,l}$ средством защиты своих функций по противодействию jk-му способу реализации k угрозы объекту l. Иначе, удельная эффективность $h_{i,\,jk,\,k,\,l}$ есть вероятность того, что данный способ jk реализации угрозы k объекту l будет предотвращен.

Отображение точек c и их совокупностей пространства C на пространство H осуществляется по аналитическим или экспертным оценкам:

$$c_{k,\,l} \rightarrow h_{k,\,l}$$
$$C \rightarrow H$$

Пространство оценок стоимости средств противодействия $\Psi(пси)$ содержит множество точек ψ, каждая из которых соответствует значению стоимости конкретного средства противодействия c. При этом под «стоимостью» средства противодействия следует подразумевать как финансовые затраты, так и условные затраты.

Отображение точек c пространства C на пространство Ψ осуществляется по аналитическим или экспертным оценкам:

$$c_{k,\,l} \rightarrow \psi_{k,\,l}$$
$$C \rightarrow \Psi$$

Пространство решений A состоит из элементов a, которые представляют собой решения на основе возможных воздействий источников угроз k на объект защиты l и применения имеющихся средств защиты c. Алгоритмом решения является решающая функция $D\ (a/к,\ c)$, определенная на пространствах $K,\ V,\ L,\ C,\ H$ и Ψ и принимающая значение из A. Решающая функция осуществляет отображение точек из пространства источников угроз K, пространства информационных объектов L и пространства средств защиты C в пространство решений A. Это отображение носит вероятностный характер, т.е. для каждого $k\ (jk)$ и $c_{i,\,jk,\,k,\,l}$ будет существовать функция плотности вероятности $D\ (a/jk,\ c_{i,\,jk,\,k,\,l})$ из пространства решений A.

Разделим пространство А на 5 подпространств.

В подпространстве A^{w1} будут находиться точки a_1, определяющие решающую функцию, которая представляет собой алгоритм работы i-го средства противодействия $c_{i,\ jk,\ k,\ l}$ конкретному способу jk реализации определенной угрозы k объекту защиты l:

$$a_1 \rightarrow D\ (a/jk,\ c_{i,\ jk,\ k,\ l}) = D\ (a/jk) \wedge D\ (a/\ c_{i,\ jk,\ k,\ l}).$$

В подпространстве A^{w2} будут находиться точки a_2, определяющие решающую функцию, которая представляет алгоритм организации работы всех средств противодействия $c_{jk,\ k,\ l}$ конкретному способу jk реализации определенной угрозы k объекту l:

$$a_2 \rightarrow D\ (a/jk,\ c_{jk,\ k,\ l}) = D\ (a/jk) \wedge D\ (a/\ c_{jk,\ k,\ l}).$$

В подпространстве A^{w3} будут находиться точки a_3, определяющие решающую функцию, которая представляет алгоритм реализации и координации действий всех средств противодействия $c_{k,\ l}$ всем способам реализации угрозы k объекту l:

$$a_3 \rightarrow D\ (a/k,\ c_{k,\ l}) = D\ (a/k) \wedge D\ (a/\ c_{k,\ l}),$$

для всех $j \subset J$.

В подпространстве A^{w4} будут находиться точки a_4, определяющие решающую функцию, которая представляет алгоритм реализации и координации действий всех средств противодействия c_1 от всех предполагаемых угроз объекту l:

$$a_4 \rightarrow D\ (a/k,\ c_{k}) = D\ (a/k) \wedge D\ (a/\ c_{l}),$$

для всех $k \subset K$.

В подпространстве A^{w5} будут находиться точки a_5, определяющие решающую функцию, которая представляет алгоритм реализации и координации действий всех средств противодействия C от всех предполагаемых угроз k для всех объектов защиты l:

$$a_5 \rightarrow D\ (a/K,\ C) = D\ (a/K) \wedge D\ (a/C),$$

Таким образом, решающая функция D (a/k, c) вместе с пространствами A, K, V, L, C, H и Ψ образует математическую модель процесса защиты информации.

Исходя из всего вышесказанного, можно сделать, что общая математическая модель является лучшей из предложенного списка, так как обладает высокой эффективностью, универсальностью и огромным потенциалом применения на практике. Можно сказать, что метод объединяет основные принципы остальных мат. методов. Безусловно, развернутость данного метода будет отрицательно влиять на скоротечность процесса вычисления риска угрозы безопасности АИС, поэтому в некоторых случаях рекомендуется прибегнуть к другим методам, которые не являются настолько подробными.

Библиографический список

1. ГОСТ Р 50922-96. Государственный Стандарт Российской Федерации. Защита информации. Основные термины и определения. – М., 1996.

2. Росенко, А.П. «Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе» / А.П. Росенко // Известия Южного федерального университета. Технические науки. – 2008. – Вып. 8. – С. 71–81.

3. Лекция 5. «Экономика безопасности на примере оценки криптосистем» // ИНТУИТ. – URL: http://www.intuit.ru/studies/courses/600/456/lecture/10199. – С. 2.

4. Костин, Н.А. Общая математическая модель защиты информации / Н.А. Костин // Информационное общество. – 1996. – Вып. 6. – С. 13–25.

К содержанию