УДК 614.2

С.К. Варлатая, М.В. Шаханова

Математические модели динамики возникновения и реализации угроз информационной безопасности

Необходимость разработки математических моделей динамики возникновения и реализации угроз безопасности информации в информационных системах обусловлена важностью учета фактора времени при технической ЗИ и корректной оценке ее эффективности. Вместе с тем применительно к технической ЗИ в информационных системах, где превалирует качест-венный подход к анализу угроз безопасности информации, математические модели динамики их возникновения и реализации практически не разрабатывались. С учетом этого рассмотрим подход к разработке указанных моделей, основанный на теории потоков [1, 2], и к оценке возможности возникновения и реализации угроз с использованием вероятностных показателей.

Ключевые слова: угрозы информационной безопасности, потоки угроз, пуассоновский поток.

Динамика возникновения и реализации угрозы включает в себя два последовательных процесса возникновения угрозы и реализации этой угрозы. При этом возникновение угрозы может определяться динамикой появления источников угроз или, если источник постоянно присутствует, динамикой возникновения определенной совокупности существенных факторов, определяющих появление угрозы.

Продолжительность существования угрозы определяется содержанием самой угрозы, длительностью существования источника угрозы или факторов, определяющих наличие угрозы.

Возможность реализации угрозы обусловлена, во-первых, фактом наличия угрозы, во-вторых, временем, прошедшим с момента возникновения угрозы, в-третьих, характеристиками угрозы, объекта информатизации (информационной системы), а также техническими условиями реализации угрозы. Реализация угрозы является процессом, происходящим в ограниченное время с определенной вероятностью. При этом угрозы могут быть следующими:

а) без последействия, когда их реализация приводит к немедленным негативным последствиям;

б) с ограниченным последействием, когда момент начала реализации угрозы определяется временем возникновения некоторого события, происходящего, как правило, независимо от наличия угрозы, с последующими немедленными негативными последствиями;

в) с последействием, когда негативные последствия реализации угрозы наступают через определенный (детерминированный или статистически устойчивый) промежуток времени.

Если угроза реализована, то это не означает, что она перестает существовать. На объекте информатизации может существовать множество угроз безопасности информации. Если рассматривать это множество во времени, то оно является открытым, состоящим из подмножеств однородных (подобных) угроз. Угрозы считаются однородными, если они порождены одним и тем же или сходным источником угроз, адекватны по содержанию и способны вызвать одинаковые негативные последствия. Каждое подмножество однородных угроз представляет собой во времени поток однородных угроз. Потоки, представляющие разные подмножества, могут существовать одновременно. Таким образом, можно рассмотреть три возможных на практике случая, на основе которых строится различный математический аппарат моделей динамики возникновения и реализации угроз информационной безопасности.

1. Потоки разнородных угроз являются независимыми друг от друга, угрозы, принадлежащие одному потоку, появляются последовательно в независимые моменты времени. Появление каждой угрозы описывается временем ее появления и временем существования. Это позволяет представить поток однородных угроз во времени в виде потока прямоугольных импульсов, момент появления которого соответствует моменту появления угрозы, а длительность – продолжительности существования данной конкретной угрозы.

Пусть t_1, t_2, ... – моменты появления угроз безопасности информации, при этом $t_{k-1} \geq t_k$, $k \geq 1$, а τ_1, τ_2 – длительности существования угроз. Положим $z_k = t_k - t_{k-1}$, $k \geq 1$, $t_0 = 0$. Тогда поток однородных событий считается заданным, если заданы независимые распределения случайных векторов $Z = \{z_1, z_2, ...z_n\}$ и $T = \{\tau_1, \tau_2, ...\tau_n\}$. Определяющим для оценки возможности возникновения данного вида угрозы (из данного подмножества однородных угроз) является распределение вектора *Z*. Как правило, случайные величины z_1, z_2,…, z_n – независимы, и поток однородных событий является потоком с ограниченным последействием [3], для которого достаточно задать лишь функции распределения каждой из указанных величин $f(z_1)$, $f(z_2)$,…, $f(z_n)$. Тогда в качестве показателя возможности появления на заданном промежутке времени данного вида угрозы можно использовать вероятность появления хотя бы одной угрозы из потока за заданное время. Если поток угроз является рекуррентным [3], то эта вероятность определяется из следующего соотношения:

$$P_{ap}(t) = \mu \int_0^t [1 - f(z)] dz, \quad (1)$$

где μ – средняя интенсивность потока угроз.

Как правило, для оценочных расчетов вполне приемлемым является допущение о пуассоновском характере потока угроз, когда $f(z) = 1 - \exp(-\mu t)$, при этом вероятность появления угрозы рассчитывается по аналогичной формуле:

$$P_{ap}(t) = 1 - \exp(-\mu t). \quad (2)$$

Для расчета по формуле (2) достаточно задать расчетное время и интенсивность появления угроз данного класса (интенсивность однородных угроз).

2. Однородные угрозы возникают лишь в некоторые «вызывающие» случайные промежутки времени, в остальное время существование угроз невозможно.

В этом случае поток угроз может быть представлен в виде потока пачек импульсов, в котором поток огибающих равнозначен рекуррентному потоку «вызывающих» промежутков времени, а поток внутри этих промежутков соответствует собственно потоку угроз (рис. 1).

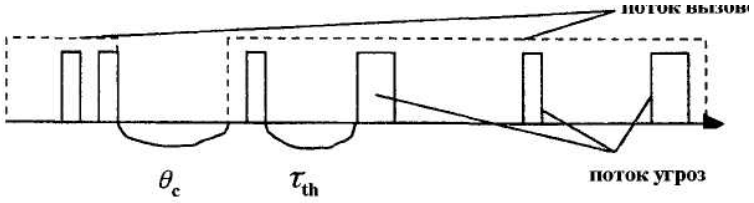

Рис. 1. Поток угроз в «вызывающие» промежутки времени

Плотность распределения вероятности для суммы τ случайных независимых величин $\theta_в$ и τ_y определяется из следующего соотношения:

$$w(t) = \int_0^\tau w_c(\theta_c) w_{th}(\tau - \theta_c) d\theta_c, \quad (3)$$

где $\tau = \theta_c + \tau_{th}$ – время до появления первой угрозы; $w_c(\theta_c)$ – плотность распределения вероятности для длительности паузы между пачками импульсов («вызовами»); $w_{th}(\tau_{th})$ – плотность распределения вероятности для времени до появления первой угрозы в пачке.

Вероятность того, что хотя бы одна угроза появится в течение времени *t*, определяется по формуле

$$P_{ap}(t) = \int_0^\tau w(\tau) d\tau. \quad (4)$$

Как правило, для оценки этой вероятности оказывается приемлемым пуассоновское распределение [2, 3] случайных величин τ и τ_{th}, при этом указанная вероятность рассчитывается по формуле

$$P_{ap}(t) = 1 - \frac{1}{\mu_{th} - \mu_c} [\mu_{th} \exp(-\mu_c t) - \mu_c \exp(\mu_{th} t)], \quad (5)$$

где μ_{th} и μ_c – интенсивности соответственно потоков угроз и промежутков времени, в которые они могут существовать.

3. Потоки однородных угроз возникают в одни и те же промежутки времени, при этом появляется либо один из потоков угроз с определенной вероятностью, либо несколько потоков разнородных угроз.

Пусть в некоторые случайные промежутки времени могут существовать J потоков угроз, при этом вероятность существования j-го потока ($j=\overline{1,J}$) для разных промежутков времени одинакова и составляет величину p_j. Поток промежутков времени, когда могут существовать угрозы, является пуассоновским с интенсивностью μ_c, а потоки угроз внутри этих промежутков времени – пуассоновскими с интенсивностями μ_{thj}. Суммарная интенсивность потока разнородных угроз в пределах случайного промежутка времени определяется соотношением

$$\mu_\Sigma = \sum_j p_j \mu_{thj} . \tag{6}$$

Тогда вероятность появления хотя бы одной из разнородных угроз за время t рассчитывается по формуле (5), где вместо μ_{th} необходимо подставить μ_Σ, а вероятность появления угрозы из j-го потока однородных угроз – по формуле (2), где вместо μ подставляется μ_Σ.

Следует отметить, что суммарный поток неоднородных угроз может быть неординарным, т.е. в одно и то же время может существовать несколько разнородных угроз (импульсы, описывающие потоки разнородных угроз, накладываются друг на друга). При детальном анализе динамики возникновения разнородных угроз рассматриваются возможности совпадения как части (k из n, $k=\overline{1,n}$) разнородных угроз, так и всей ($I^{(p)}$ – из n) совокупности таких угроз. Интенсивность совпадений k импульсов из n потоков появления во времени разнородных угроз при длительности совпадения не менее δ выражается в виде [2]

$$\mu_{n,k}(\delta) = -\frac{1}{k!}\frac{\partial^{k+1}}{\partial\lambda^k \partial\delta}\prod_{s=1}^{n}[Q_s(\delta)+\lambda P_s(\delta)]_{\lambda=0} , \tag{7}$$

где $P_s(\delta) = \mu_s \int_0^\infty dx \int_x^\infty w_{ts}(y)dy$ – вероятность того, что произвольно выбранная точка на временной оси окажется в пределах укороченного на величину δ импульса s-го потока; $w_{ts}(y)$ и $w_{\theta s}(y)$ – плотности распределения вероятности для длительности импульса и паузы между импульсами s-го потока; $Q_s(\delta) = \mu_s \int_0^\infty dx \int_x^\infty w_{\theta s}(y)dy$ – вероятность того, что произвольно выбранная точка на временной оси окажется в пределах укороченной на величину δ паузы между импульсами s-го потока.

В частности, для экспоненциальных законов распределения длительности импульсов и пауз средняя вероятность появления импульсов совпадения всех n потоков разнородных угроз в пределах промежутка времени, когда эти угрозы могут иметь место, определяется как [3]

$$\overline{P_n} = \frac{1}{\tau_c}\int_0^\infty [1-(1-\prod_{s=1}^{n}\mu_s\tau_s)\exp(-\frac{x}{\theta_{nn}})]\exp(-\frac{x}{\tau_s})dx , \tag{8}$$

где τ_s – средняя продолжительность промежутка времени существования угроз; θ_{nn} – средняя продолжительность паузы между импульсами потока совпадений,

$$\theta_{nn} = \frac{1-\prod_{s=1}^{n}\mu_s\tau_s}{\mu_{nn}} . \tag{9}$$

Вероятность того, что за время t появится импульс потока совпадений, рассчитывается по формуле

$$P_{ap}(t) = 1 - \frac{1}{\mu_{nn}\overline{P_n}-\mu_c}[\mu_{nn}\overline{P_n}\exp(-\mu_c t) - \mu_c \exp(-\mu_{nn}\overline{P_n}t)] . \tag{10}$$

На практике может иметь место любой из описанных трех случаев. Поэтому для каждого вида угроз в соответствии с предложенным подходом должна разрабатываться адекватная математическая модель динамики их возникновения на объекте информатизации. Предложенные вероятностные показатели позволяют оценить возможность возникновения угроз в заданный промежуток времени.

Возникшая угроза может быть реализована при определенных условиях. Процесс реализации угроз, как правило, является случайным. Рассмотрим методический подход к формализации динамики реализации угроз безопасности информации.

Методический подход к формализации математических моделей динамики реализации угроз в компьютерной системе основывается на изложенном выше подходе к описанию динамики их возникновения и аппарате теории стохастических систем массового обслуживания [3]. Суть его состоит в следующем.

Угроза может реализовываться по одному из трех вариантов сценариев:

1) в течение времени существования угрозы;

2) с момента инициализации ассоциированного с угрозой события (например, при запуске какой-то определенной программы);

3) через некоторый случайный промежуток времени, необходимый для формирования условий для реализации угрозы (например, через промежуток времени, необходимый для проникновения вируса к серверу или коммуникационному элементу сети).

В первом варианте, когда угроза реализуется в течение времени ее существования, динамика реализации может быть описана следующим образом. Поток импульсов, описывающий динамику появления однородных угроз безопасности информации, прореживается со средней вероятностью реализации угроз в компьютерной системе $\overline{P_{\text{real}}}$ за время ее существования [3]:

$$\overline{P_{\text{real}}} = \int_0^\infty P_{\text{real}}(\tau_{th}) w_{th}(\tau_{th}) d\tau_{th}, \tag{11}$$

а для экспоненциального распределения длительности существования однородных угроз

$$\overline{P_{\text{real}}} = \frac{1}{\overline{\tau_{th}}} \int_0^\infty P_{\text{real}}(\tau_{th}) \exp(-\frac{\tau_{th}}{\overline{\tau_{th}}}) d\tau_{th}. \tag{12}$$

В этом случае необходимо знать зависимость вероятности реализации угрозы от времени в данной компьютерной системе и плотность распределения вероятности длительности существования данного вида угрозы. В настоящее время практически отсутствуют аналитический аппарат и статистические данные для определения этих величин. Для получения зависимостей вероятности реализации угрозы от времени для некоторых видов угроз мог бы быть использован подход, основанный на определении среднестатистических значений времени реализации тех или иных угроз. Вместе с тем реализация некоторых угроз не зависит от времени их существования. В этом случае необходимо иметь статистику реализации каждого вида угроз, по которой можно определить $\overline{P_{\text{real}}}$. Наиболее перспективным направлением набора такой статистики и определения указанных частных показателей для различных видов угроз является имитационное моделирование процессов реализации угроз безопасности информации, например с применением аппарата сетей Петри [4].

Во втором варианте, когда угроза реализуется с момента инициализации ассоциированного с угрозой события, необходимо знать динамику проявления этого события в данной компьютерной системе или на объекте информатизации. При этом такая динамика может быть описана потоком бесконечно коротких импульсов, основной характеристикой которого является плотность распределения вероятности для случайного периода следования этих импульсов. Пусть динамика инициализации события, ассоциированного с *j*-й угрозой, описывается плотностью $w_{T_{j\text{seq}}}(T_{j\text{seq}})$, при его инициализации угроза реализуется с единичной вероятностью, рассматривается ординарный поток однородных угроз, и $\tau_j = T_{j\text{seq}} + \theta_j$ – время, соответствующее сумме длительности паузы до появления первой угрозы в потоке и периода инициализации ассоциированного события. Плотность распределения вероятности для случайной величины τ_j определяется соотношением

$$w(\tau_j) = \int_0^\infty w_{th}(\theta_{th}) w_{T_{j\text{seq}}}(T_{j\text{seq}} - \theta_j) d\theta_j. \tag{13}$$

Тогда вероятность того, что за время *t* угроза появится и будет реализована, рассчитывается при условии экспоненциального распределения инициализаций ассоциированного события и пуассоновского потока угроз следующим образом:

$$P_{\text{real}}(t) = 1 - \frac{\overline{T_{j\text{seq}}}\,\overline{\theta_j}}{\overline{T_{j\text{seq}}} - \overline{\theta_j}} [\overline{\theta_j} \exp(-\overline{T_{j\text{seq}}} t) - \overline{T_{j\text{seq}}} \exp(-\overline{\theta_j} t)], \tag{14}$$

где $\overline{T_{j\text{seq}}}$ и $\overline{\theta_j}$ – средние значения периода следования потока инициализаций и паузы между однородными угрозами в *j*-м потоке.

Аналогичным образом могут быть получены соотношения в случаях, когда однородные угрозы возникают лишь в некоторые случайные промежутки времени, а в остальное время существование угроз невозможно, и когда часть потоков разнородных угроз возникает в одни и те же промежутки времени, при этом имеет место либо один поток однородных угроз с определенной вероятностью, либо несколько потоков разнородных угроз.

В третьем варианте угроза реализуется через некоторый промежуток времени с момента возникновения. Время реализации характеризуется плотностью распределения вероятности w_{real}, (T_{real}). В этом случае соотношения для расчета вероятности появления и реализации угрозы за заданное время аналогичны (14) с той лишь разницей, что вместо периода инициализации $\overline{T_{j\text{seq}}}$ подставляется среднее значение времени реализации $\overline{T_{\text{real}}}$.

Предложенные математические модели и методический подход для описания динамики возникновения и реализации угроз информационной безопасности позволяет учесть влияние мер технической ЗИ. Для этого вводятся дополнительные параметры, определяющие снижение интенсивности возникновения угроз, если предпринимаемые меры ЗИ являются превентивными, либо увеличение времени, необходимого на реализацию угрозы ($\overline{P_{\text{real}}}$ или $\overline{T_{j\text{seq}}}$), либо уменьшение средней вероятности $\overline{P_{\text{real}}}$.

В случае отсутствия возможности набора состоятельной статистики возможно применение аппарата теории нечетких множеств для формирования функций принадлежности и замены вероятностей и параметров, учитывающих влияние мер ЗИ, на соответствующие количественные характеристики (лингвистические переменные), формируемые на основе нечетких высказываний экспертов [5].

Литература

1. Большаков И.А. Прикладная теория случайных потоков / И.А. Большаков, В.С. Ракоишц. – М.: Сов. радио, 1978. – 248 с.

2. Сухарев Е.М. Модели технических разведок и угроз безопасности информации. – М.: Радиотехника, 2003. – 144 с.

3. Климов Г.П. Стохастические системы обслуживания. – М.: Наука, 1966. – 243 с.

4. Питерсон Дж. Теория сетей Петри и моделирование систем. – М.: Мир, 1984. – 264 с.

5. Кофман А. Введение в теорию нечетких множеств. – М.: Радио и связь, 1982. – 432 с.

Варлатая Светлана Климентьевна
Канд. техн. наук, доцент каф. информационной безопасности
Дальневосточного федерального университета (ДВФУ)
Тел.: 8-924-244-40-33
Эл. почта: sk-varl@yandex.ru

Шаханова Марина Владимировна
Ст. преподаватель каф. информационной безопасности ДВФУ
Тел.: 8-914-735-70-19
Эл. почта: marinavl2007@yandex.ru

Varlataya S.K., Shakchnova M.V.

Mathematical models of the dynamics of the emergence and implementation of information security threats

The need to develop mathematical models of the dynamics emergence and implementation of information security threats in information systems, due to the importance of taking into account the time factor, with technical data protection and correct assessment of its efficiency. At the same, in the case of the technical data protection in information systems, where the prevailing qualitative approach to the analysis of information security threats , and mathematical models of the dynamics of their emergence and implementation of practically not designed. With this in mind, consider the approach to the development of models based on the theory of streams [1, 2], and to assess the feasibility of emergence and implementation threats using indicators of probability.

Keywords: information security threats, streams of threats, Poisson process.