УДК 621.391.16

ДИНАМИКА УЯЗВИМОСТЕЙ В СОВРЕМЕННЫХ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

А. С. Вялых, С. А. Вялых

Воронежский государственный университет

Поступила в редакцию 21.04.2011 г.

Аннотация. В статье описывается новый подход к определению потенциальной вероятности защищенности современных информационных систем.
Ключевые слова: уязвимость, информационная система, несанкционированный доступ, система массового обслуживания, сеть массового обслуживания.
Annotation. In article we consider the new approach to determination of potential probability of security of the modern information systems.
Keywords: vulnerability, information system, illegal access, queuing system, network of mass service.

Построение современных защищенных информационных систем (ИС) требует учета всех возможных угроз безопасности информации, что предполагает полное и точное их описание. В течение долгого времени исследования в данном направлении носили закрытый характер, и только недавно была опубликована «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [1], в которой авторы предприняли попытку формально описать все возможные угрозы несанкционированного доступа (НСД). Модель классифицирует и описывает угрозы по 5 основным параметрам (источник угрозы, уязвимость программного или аппаратного обеспечения, способ реализации угрозы, объект воздействия, деструктивное действие), однако она не в полной мере учитывает жизненный цикл ИС и динамику изменения ее уязвимостей. Статистика компании Майкрософт [2], показывающая, что темпы закрытия уязвимостей в современных ИС часто могут отставать от скорости их обнаружения, указывает на существенность этого недостатка и на необходимость дополнительного исследования данного вопроса.

К настоящему времени уже опубликован ряд статей, освещающих эту тему. В частности, в [3] предлагается представить процесс появления новых уязвимостей и их устранения в виде работы системы массового обслуживания (СМО), на вход которой поступает пуассоновский поток заявок (уязвимостей) с интенсивностью λ, и далее СМО обслуживает эти заявки (устраняет уязвимости) с интенсивностью μ. Кроме того, предполагается, что работа над устранением каждой уязвимости начинается сразу же после ее обнаружения, соответственно данная СМО имеет бесконечное число каналов обслуживания. В данных предположениях вероятность того, что в системе отсутствуют уязвимости, получилась равной [3]:

$$P(0) = \frac{1}{1 + \sum_{n=1}^{\infty} \frac{1}{n!} \left(\frac{\lambda}{\mu} \right)^n}, \lambda > 0, \mu > 0. \qquad (1)$$

Можно показать, что с учетом формулы [4]:

$$e^x = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}, \qquad (2)$$

выражение (1) принимает вид:

$$P(0) = e^{-\frac{\lambda}{\mu}}, \lambda > 0, \mu > 0.. \qquad (3)$$

В предложенной модели предполагается, что уязвимость может находиться в 3-х состояниях: либо быть неизвестной, либо быть известной и незакрытой, либо быть известной и закрытой. В действительности состояние, когда уязвимость известна и незакрыта, можно поделить на несколько разных состояний. В частности предлагается рассматривать следующие состояния: уязвимость известна ограниченному кругу лиц, уязвимость опубликована в открытых источни-

ках, на уязвимость выпущен патч, закрывающий ее. Введение данных состояний существенным образом меняет математическую модель, описывающую динамику уязвимостей в системе, а именно СМО расширяется до сети массового обслуживания (СеМО), состоящей из 4-х СМО, каждая из которых имеет бесконечное число каналов (рис. 1).

На вход данной сети поступает поток заявок (уязвимостей) с интенсивностью λ. Под заявками, еще не поступившими в СеМО, подразумеваются неизвестные уязвимости. Предполагается, что число таких уязвимостей бесконечно. Процесс поступления заявок в систему имитирует процесс обнаружения уязвимостей. Далее поток заявок разделяется на два. С вероятностью $1\text{-}P_{согл}$ заявки поступают в систему массового обслуживания №1 и с вероятностью $P_{согл}$ в систему массового обслуживания №2. $P_{согл}$ – это вероятность того, что раскрытие уязвимостей будет согласованным, то есть конфиденциальным раскрытием уязвимостей соответствующему поставщику, чтобы он мог разработать исчерпывающее обновление безопасности для устранения уязвимости до того, как о ней станет широко известно [2]. Соответственно, входящий поток заявок в СМО №2 представляет собой согласованное раскрытие уязвимостей. Общее количество заявок в СМО №1 и СМО №2 равно количеству незакрытых уязвимостей, известных ограниченному кругу лиц. Работа системы массового обслуживания №1 имитирует процесс публикации уязвимостей, известных ограниченному кругу лиц, в открытых источника. Данная СМО обслуживает каждую заявку (уязвимость) с интенсивностью μ_1, а n_1 - число заявок в этой СМО. Работа системы массового обслуживания №2 имитирует процесс выпуска патчей, закрывающих уязвимости, известные ограниченному кругу лиц. Данная СМО обслуживает каждую заявку (уязвимость) с интенсивностью μ_2, а n_2 - число заявок в этой СМО. Из СМО №1 заявки с вероятностью, равной 1, поступают в СМО №3, работа которой имитирует процесс выпуска патчей на уязвимости, опубликованные в открытых источниках. Данная СМО обслуживает каждую заявку (уязвимость) с интенсивностью μ_3, а n_3 - число заявок в этой СМО. Количество заявок в СМО №3 равно количеству незакрытых уязвимостей, опубликованных в открытых источниках. Из СМО №2 и СМО №3 заявки с вероятностью, равной 1, поступают в СМО №4, работа которой имитирует процесс закрытия уязвимостей в системе при помощи установки соответствующих патчей. Данная СМО обслуживает каждую заявку

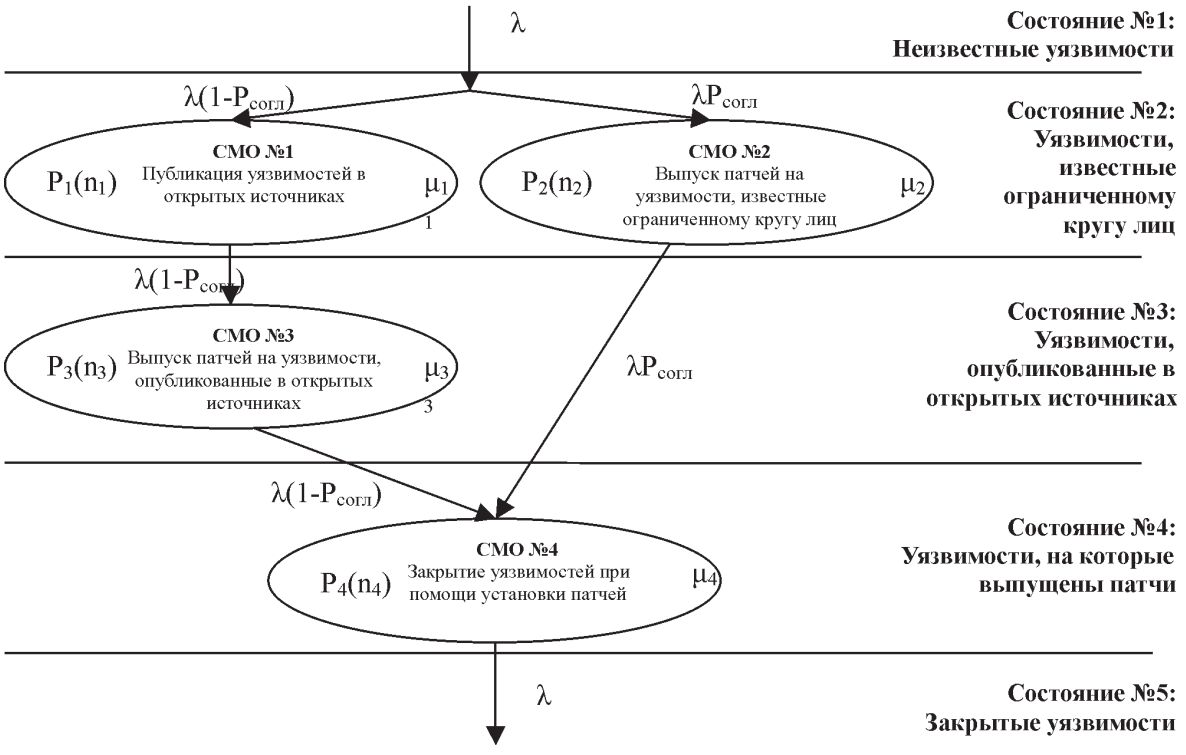

Рис. 1. Динамика уязвимостей в информационной системе

(уязвимость) с интенсивностью μ_4, а n_4 - число заявок в этой СМО. Количество заявок в СМО №4 равно количеству незакрытых уязвимостей, на которые выпущены патчи. Под заявками, вышедшими из СеМО, подразумеваются закрытые уязвимости. По аналогии с [3] считается, что ИС полностью защищена, если в ней отсутствуют известные незакрытые уязвимости (состояния 2-4) и полностью незащищена, если в ней есть хотя бы одна незакрытая уязвимость, кроме того, так же, как и в [3], предполагается, что в системе установился стационарный режим, и поток заявок, входящий в любую СМО, равен потоку заявок, выходящему из этой СМО. Вероятность отсутствия уязвимостей в ИС будет равна вероятности отсутствия в СеМО заявок.

Вероятность того, что в СеМО, состоящей из M СМО, находится n заявок, можно рассчитать по формуле [7]:

$$P(n) = \prod_{i=1}^{M} P_i(n_i), \ \sum_{i=1}^{M} n_i = n, \qquad (4)$$

где $P_i(n_i)$ – вероятность того, что в i-й СМО будет n_i заявок. В случае M=4, вероятность того, что в СеМО отсутствуют заявки, рассчитывается по формуле:

$$P(0) = P_1(0)P_2(0)P_3(0)P_4(0), \qquad (5)$$

Вероятность того, что в i-й системе находится n_i заявок, равна [7]:

$$P_i(n_i) = P_i(0)\frac{\rho_i^{n_i}}{\beta_i(n_i)}, \ i = \overline{1,M}, \qquad (6)$$

где $P_i(0)$ – вероятность того, что в i-й системе отсутствуют заявки.

$$\rho_i = \frac{\lambda_i}{\mu_i}, \qquad (7)$$

где λ_i – интенсивность потока заявок, входящего в i-ю СМО, а μ_i – интенсивность их обработки в этой СМО [7].

$$\beta_i(n_i) = \begin{cases} n_i!, n_i = \overline{0,c_i} \\ c_i!\, c_i^{n_i - c_i}, n_i \geq c_i \end{cases}, \qquad (8)$$

где c_i – число каналов обработки в i-й СМО [7].

При использовании свойства $\sum_{n_i=0}^{\infty} P_i(n_i) = 1$, $n_i \geq 0$, $i = \overline{1,M}$ [5], получается:

$$P_i(0) = \frac{1}{\sum_{n_i=0}^{\infty} \frac{\rho_i^{n_i}}{\beta_i(n_i)}}, \ n_i \geq 0, \ i = \overline{1,M}. \qquad (9)$$

Так как число каналов обработки в каждой СМО бесконечно ($c_г = \infty$), то

$$\beta_i(n_i) = n_i!, \qquad (10)$$

а вероятность отсутствия заявок в i-й СМО рассчитывается по формуле:

$$P_i(0) = \frac{1}{\sum_{n_i=0}^{\infty} \frac{1}{n_i!}\left(\frac{\lambda_i}{\mu_i}\right)^{n_i}}. \qquad (11)$$

Или, при упрощении, используя формулу (2), получается:

$$P_i(0) = e^{-\frac{\lambda_i}{\mu_i}}. \qquad (12)$$

Интенсивность входящего в i-ю СМО потока равна [7]

$$\lambda_j = \lambda_0 a_j + \sum_{i=1}^{M} \lambda_i \Theta_{ij}, \ j = \overline{1,M}, \qquad (13)$$

где $\vec{\alpha}$, вектор, распределяющий вызовы поступивших заявок между M узлами сети, а Θ – квазистохастическая матрица, управляющая переходами между M узлами сети после завершения обслуживания заявки в очередном узле на ее маршруте.

Для СеМО, приведенной в этой статье (рис. 1), вектор $\vec{\alpha}$ равен

$$\vec{\alpha} = \begin{bmatrix} (1 - P_{согл}) & P_{согл} & 0 & 0 \end{bmatrix}, \qquad (14)$$

а квазистохастическая матрица

$$\Theta = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \qquad (15)$$

Интенсивности входных потоков для 1,2,3 и 4 СМО будут равны соответственно

$$\lambda_1 = (1 - P_{согл})\lambda, \ \lambda_2 = P_{согл}\lambda, \\ \lambda_3 = (1 - P_{согл})\lambda, \ \lambda_4 = \lambda \qquad (16)$$

При подстановке (16) в (11), получаются формулы для вероятностей отсутствия заявок в 1,2,3 и 4 СМО соответственно:

$$P_1(0) = e^{-\frac{(1-P_{согл})\lambda}{\mu_1}}, \ P_2(0) = e^{-\frac{P_{согл}\lambda}{\mu_2}}, \\ P_3(0) = e^{-\frac{(1-P_{согл})\lambda}{\mu_3}}, \ P_4(0) = e^{-\frac{\lambda}{\mu_4}} \qquad (17)$$

При использовании (17), вероятность того, что в ИС отсутствуют известные открытые уязвимости (то есть система защищена), получается равной

$$P(0) = e^{-\left(\frac{(1-P_{согл})\lambda}{\mu_1} + \frac{P_{согл}\lambda}{\mu_2} + \frac{(1-P_{согл})\lambda}{\mu_3} + \frac{\lambda}{\mu_4}\right)}. \qquad (18)$$

Таким образом, получена модель, учитывающая дополнительные возможные состояния уязвимостей.

Не трудно показать, что модель (1,3) является частным случаем полученной модели (18). Для этого достаточно предположить, что заявки приходящие в СеМО мгновенно попадают в СМО №4, то есть интенсивности работы СМО №1, СМО №2 и СМО №3 стремятся к бесконечности. Кроме того, под работой СМО №4 в этом случае понимается не просто процесс закрытия уязвимостей с помощью установки патчей, а весь процесс устранения уязвимостей, включающий их публикацию, выпуск патчей и собственно их закрытие, соответственно интенсивность работы СМО №4 должна быть равной μ. В итоге получается, что $P_1(0) = P_2(0) = P_3(0) = 1$, соответственно $P(0) = P_4(0) = e^{-\frac{\lambda}{\mu}}$, что и доказывает утверждение.

С учетом статистики Microsoft [2] можно оценить потенциальную защищенность современных систем, не использующих средства защиты информации. Количество уязвимостей в продуктах Microsoft, обнаруженных за 2009 год, приблизительно равно 500, соответственно интенсивность входного потока равна $\lambda = \frac{500}{365}$ [2]. Количество уязвимостей в продуктах Microsoft, согласованно раскрытых за 2009 год, приблизительно равно 80% от общего числа раскрытых уязвимостей в продуктах Microsoft [2], т.е. можно положить $P_{\text{согл}} = 0.8$, а в качестве интенсивности работы СМО №1 взять $\mu_1 = \frac{500}{365}(1-0.8)$. За 2009 год было устранено приблизительно 95 уязвимостей [2]. Предлагается считать, что вероятность того, что будет разрешена согласованно раскрытая уязвимость, равна вероятности согласованного раскрытия, соответственно интенсивность работы СМО №2 равна $\mu_2 = \frac{95}{365} \times 0.8$, а интенсивность работы СМО №3 $\mu_3 = \frac{95}{365} \times (1-0.8)$. Так же учитывается, что все разрешенные уязвимости устраняются из ИС, т.е. для СМО №4 можно положить $\mu_4 = \frac{95}{365}$. Исходя из тех же данных, для формулы (3) получаются следующие значения интенсивностей: $\lambda = \frac{500}{365}$ и $\mu = \frac{95}{365}$. При подстановке данных значений в формулы (3) и (18) получаются следующие оценочные значения для вероятности защищенности систем продуктов Microsoft:

по формуле (3): $P(0)=5.2\times10^{-3}$,

по формуле (18): $P(0)=5.1\times10^{-8}$.

Вероятности в обоих случаях близки к 0, что полностью соответствует действительности, так как количество обнаруживаемых уязвимостей за один и тот же промежуток времени в несколько раз больше количества уязвимостей, на которые выпускаются патчи [2].

Для защищенных систем ситуация выглядит несколько иной, здесь количество обнаруживаемых за год уязвимостей не превышает 10 [8], также предлагается считать что на разрешение каждой уязвимости в таких системах уходит в среднем месяц и все разрешенные уязвимости устраняются из ИС. Для таких систем можно положить

$$\lambda = \frac{10}{365},\ \mu = \frac{1}{30},\ P_{\text{согл}} = 0.8,\ \mu_1 = \frac{1}{30}(1-0.8),$$

$$\mu_2 = \frac{1}{30} \times 0.8,\ \mu_3 = \frac{1}{30} \times (1-0.8),\ \mu_4 = \frac{1}{30}.$$

Вероятность защищенности таких систем равна:

по формуле (3): $P(0)=0.44$,

по формуле (18): $P(0)=0.07$.

Разница между полученными вероятностями существенна. Поэтому для учета динамики уязвимостей в особо важных системах предпочтительней использовать вышеописанный подход. Полученная вероятность защищенности ИС является потенциальной, так как предложенная модель не учитывает возможность использования обнаруженных уязвимостей на конкретном защищаемом объекте.

СПИСОК ЛИТЕРАТУРЫ

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). - ФСТЭК 2008 г. – (http://www.fstec.ru/_spravs/model.rar).

2. Microsoft Security Intelligence Report v9 // Mictosoft. – (http://www.microsoft.com/security/sir/).

3. *Щеглов А.Ю.* Безопасность современных ОС «в цифрах» - (http://www.itsec.ru/articles2/Inf_security/bezopasnost-OS).

4. Основы математического анализа : Учебник для физ. специальностей и специальности "Прикладная математика" ун-тов / В. А. Ильин, Э. Г. Поз-

няк. — М. : Наука, 1980. — (Курс высшей математики и математической физики / под ред. А.Н. Тихонова [и др.] ; Вып. 2) .Ч. 2 .— 1980 .— 447 с.

5. Leta о киберпреступности в России [Электронный ресурс] / «Лаборатория Касперского». – http://live.xakep.ru/blog/kaspersky_lab/592.html.

6. *Вентцель Е. С.* Теория случайных процессов и ее инженерные приложения. – Учеб. пособие для втузов. – 2-е изд. / Е. С. Вентцель, Л. А. Овчаров. – М.: Высш. шк., 2000. – 383 с.

7. *Башарин Г.П.* Лекции по математической теории телетрафика: Учеб. пособие. – М.: Изд-во РУДН, 2004. – 186 с.

8. Vulnerability Report: Cisco IOS 12.x. [Электронный ресурс] / Secunia. – http://secunia.com/advisories/product/182/?task=statistics_2009.

Вялых Александр Сергеевич – аспирант кафедры информационных систем, Воронежский государственный университет. E-mail: alexandervyalih@gmail.com.

Вялых Сергей Ариевич – кандидат технических наук, доцент кафедры информационных систем, Воронежский государственный университет. E-mail: vyalyh@govvrn.ru.

Vyalih A. S. – post-graduate student, department of information systems, Voronezh State University. E-mail: alexandervyalih@gmail.com.

Vyalih S. A. – Cand.Tech.Sci., senior lecturer, department of information systems, Voronezh State University. E-mail: vyalyh@govvrn.ru.