П. А. Демин

КРИТЕРИИ ПОВЫШЕНИЯ ОПЕРАЦИОННОЙ УСТОЙЧИВОСТИ БИЗНЕС-ПРОЦЕССОВ В УСЛОВИЯХ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методики оценки и управления рисками, лежащие в основе систем управления информационной безопасностью, не могут гарантировать полную защиту информации организаций в силу объективных причин. К тому же их эффективное применение затруднительно в силу множества факторов и ограничений. Во-первых, оценка рисков без доверенного источника многолетней статистики, скорее всего, даст некорректные прогнозы, весьма трудоемка и отнимает значительные ресурсы и время, предъявляет высокие требования к компетенции экспертов, которая зачастую отсутствует, проводится периодически и может быстро устаревать. Во-вторых, принятие решений о мерах реагирования на риск основано на полученной величине уровня риска и объема ресурсов, требуемых для снижения риска до приемлемого уровня. В связи с этим в большинстве случаев меры реагирования ранжируются в порядке простоты их снижения, что обосновывается повышением значения величины возврата инвестиций, таким образом, организации склонны контролировать риски, которые они могут контролировать. Общая степень подверженности угрозам может оставаться прежней, при этом процесс управления рисками вселяет ложную уверенность в том, что организация в безопасности.

Очевидно, что помимо проведения мероприятий по управлению рисками организация должна обеспечить готовность к функционированию в условиях реализации угроз ИБ. Именно от способности обеспечить непрерывность своей деятельности во многом зависит общий уровень операционной устойчивости организации. Под операционной устойчивостью при этом подразумевается состояние, при котором достигаются следующие четыре цели:

1. Предупреждение воздействия операционных рисков в отношении критических процессов.

2. Поддержание функционирования критических процессов в случае наступления неблагоприятных событий.

3. Эффективное разрешение последствий реализации неблагоприятных событий и возврат к состоянию нормального функционирования процессов.

4. Совершенствование способов достижения перечисленных целей [1].

Состояние операционной устойчивости организации зависит от происходящих событий, таких как событие безопасности, инцидент, реагирование, восстановление и т. д. Функционирование системы обеспечения операционной устойчивости (далее — системы) может быть описано с помощью сети Петри C_f с нечеткой маркировкой (НСП).

Структура предлагаемой НСП представлена на рис. 1.

Нечеткая сеть Петри C_f определяется как $C_f = (N, f, \lambda, m_0)$ [2], где

1. $N = (P, T, I, O)$ — структура НСП C_f, для которой $P = \{p_1, p_2, ..., p_n\}$ — непустое конечное множество позиций; $T = \{t_1, t_2, ..., t_n\}$ — непустое конечное множество переходов ($P \cap T = \theta$); $I : P \times T \to \{0,1\}$ — входная функция переходов; $O : T \times P \to \{0,1\}$ — выходная функция переходов;

2. $f = (f_1, f_2, ..., f_n)$ — вектор значений функции принадлежности нечеткого срабатывания переходов, при этом $f_k \in [0,1] (k = 1, ..., m)$;

3. $\lambda = (\lambda_1, \lambda_2, ..., \lambda_m)$ — вектор значений порога срабатывания переходов, при этом $\lambda_k \in [0,1]$ (k=1, ..., m);

4. $m_0 = (m_1^0, m_2^0, ..., m_n^0)$ — вектор начальной маркировки, каждая координата которого определяется значением функции принадлежности нечеткого наличия одного маркера в соответствующей позиции данной НСП C_f.

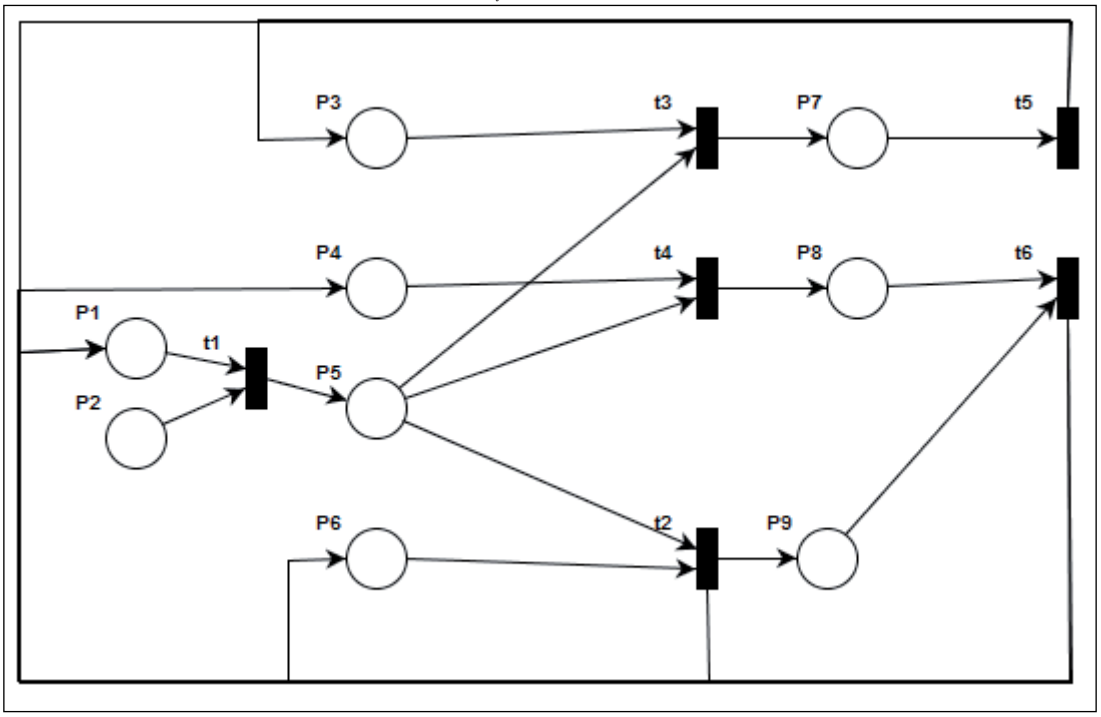

Рис. 1. Сеть Петри с нечеткой разметкой

Динамика изменения начальной и последующих маркировок НСП C_f после момента ее запуска подчиняется следующим правилам [2]:

1. Определение текущей маркировки. Любое текущее состояние НСП C_f определяется вектором $m = m_1, m_2, ..., m_n$, компоненты $m_i \in [0,1]$ которого интерпретируются как значения функции принадлежности нечеткого наличия одного маркера в соответствующих позициях $p_i \in P$ НСП C_f. Начальное состояние НСП C_f определяется вектором начальной маркировки m_0.

2. Условие активности перехода. Переход $t_k \in T$ НСП C_f является активным при некоторой текущей маркировке m, если выполнено следующее условие: $\min\limits_{(i \in \{1,2,...,n\}) \wedge (I(p_i,t_k)>0)} \{m_i\} > \lambda_k$, где λ_k — значение порога срабатывания перехода $t_k \in T$.

3. Нечеткое срабатывание перехода. Если переход $t_k \in T$ НСП C_f является активным при некоторой текущей маркировке $m_q = (m_1^q, m_2^q, ..., m_n^q)$, то нечеткое срабатывание данного перехода приводит к новой маркировке $m_{q+1} = (m_1^{q+1}, m_2^{q+1}, ..., m_n^{q+1})$, компоненты вектора которой определяются по следующим формулам:

- для каждой из входных позиций $p_i \in P$, для которых $I(p_i, t_k) > 0$: $m_i^{q+1} = 0$;
- для каждой из выходных позиций $p_j \in P$, для которых $O(t_k, p_j) > 0$:

$$m_j^{q+1} = \max\{m_j, \min\limits_{(i \in \{1,2,...,n\}) \wedge (I(p_i,t_k)>0)} \{m_i, f_k\}\},$$

где f_k — значение функции принадлежности нечеткого срабатывания перехода $t_k \in T$.

Определено множество позиций сети Петри (рис. 1):

$$P = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9,\},$$

где P_1 — состояние нормального функционирования процессов; P_2 — множество случаев возникновения рисковых ситуаций; P_3 — множество событий безопасности, в отношении которых действуют контрмеры; P_4 — множество событий безопасности, в отношении которых не действуют

контрмеры; P_5 — событие безопасности; P_6 — множество событий корректного реагирования на инцидент; P_7 — состояние действия контрмеры; P_8 — состояние прерывания или деградации функционирования процессов, обусловленное инцидентом безопасности; P_9 — множество событий реализации планов реагирования на инцидент.

Определен вектор начальной маркировки: $m_0 = (m_1^0, m_2^0, ..., m_9^0)$, где $m_1^0, m_5^0, m_7^0, m_8^0$ — значения функций принадлежности наличия маркеров в позициях P_1, P_5, P_7, P_8, определяющие состояние нормального функционирования процессов, событие безопасности, состояние действия контрмеры, состояние прерывания или деградации функционирования процессов соответственно; m_2^0 — значение функции принадлежности наличия маркера в позиции P_2, т. е. вероятность наступления рисковой ситуации; m_3^0, m_4^0 — значения функций принадлежности наличия маркеров в позициях P_3, P_4, т. е. функция принадлежности возникновения событий безопасности, в отношении которых организация защищена и не защищена соответственно; m_6^0, m_9^0 — значения функций принадлежности наличия маркеров в позициях P_6, P_9, т. е. вероятность корректного реагирования на событие безопасности и вероятность успешной реализации мер реагирования.

Установлена начальная маркировка сети Петри: $m_{1,3,4}^0 = 1$; $m_{5,7,8}^0 = 0$; $f_{1-6} = 1$.

Рисковая ситуация возникает, когда изменяющиеся факторы, влияющие на состояние ИБ, принимают неблагоприятные значения. Можно привести такие примеры рисковых ситуаций, как появление злоумышленника или инфраструктурное изменение [3].

В результате рисковой ситуации может наступать событие безопасности. Согласно ГОСТ Р ИСО/МЭК 18044:2007 [4], событие безопасности определяется следующим образом: «выявленный случай системы, услуги или состояния сети, указывающий на возможное нарушение политики защиты информации или нарушения в работе средств защиты, или прежде неизвестная ситуация, которая может иметь значение для защиты».

Природа рисков такова, что одно и то же событие безопасности может приводить к разным по видам и величине ущербам. Влияние события безопасности рассматривается с учетом естественной способности процесса противостоять рисковым событиям. Такое свойство процесса называется защищенностью (или чаще обратной ей сущностью — уязвимостью) [3].

Переход t_1 происходит при условии $m_2^0 \geq \lambda_1$, т. е. в том случае, когда вероятность наступления рисковой ситуации выше порога срабатывания перехода t_1. λ_1 при этом отражает подверженность организации влиянию изменений тех или иных факторов.

В случае $m_2^0 \geq \lambda_1$ переход t_1 срабатывает, что приводит к событию безопасности и новой маркировке m_1: $m_1^1 = 0, m_2^1 = 0, m_5^1 = m_2^0$. Дальнейший анализ показывает, что переход t_3 срабатывает при условии $m_5^1 = m_2^0 \geq \lambda_3$, так как $m_3^1 = m_3^0 = 1$, а переход t_4 при условии $m_5^1 = m_2^0 \geq \lambda_4$, так как $m_4^1 = m_4^0 = 1$. Так как автора интересуют состояния системы в условиях реализации угрозы ИБ, далее анализируется второй сценарий.

Активность перехода t_4 означает, что система недостаточно резистентна к произошедшему событию безопасности, т. е. не обладает естественной способностью противостоять данному событию безопасности и не имеет в своем составе средств его нейтрализации. Срабатывание перехода t_4 приводит к инциденту безопасности. Согласно ГОСТ Р ИСО/МЭК 18044:2007 [4], инцидент безопасности — это одно или серия нежелательных или неожиданных (рисковых) событий в системе защиты информации, которые имеют большой шанс (высокую вероятность) скомпрометировать деловые операции и поставить под угрозу защиту информации. Как видно из определения, важнейшей характеристикой инцидента безопасности является его влияние на функционирование процессов.

Активность перехода t_4 приводит к новой маркировке m_2:

$$m_8^2 = \min\{m_4^1, m_5^1\} = \min\{m_4^0, m_2^0\} = m_2^0,$$

так как $m_4^0 = 1$. Таким образом, для возврата в позицию P_1, т. е. для возврата к нормальному состоянию функционирования процессов, необходимо выполнение двух условий:

1. Активность перехода t_2, т. е. выполнение условия $\min\{m_5^1, m_6^1\} = \min\{m_2^0, m_6^0\} > \lambda_2$. В этом случае срабатывание перехода t_2 приводит к новой маркировке

$m_3: m_9^3 = \min\{m_2^0, m_6^0\}$.

2. Активность перехода t_6, т. е. выполнение условия $\min\{m_8^2, m_9^3\} = \min\{m_2^0, m_6^0\} > \lambda_6$.

Анализ сети Петри и условий срабатывания переходов показал, что операционная устойчивость в условиях реализации угроз ИБ достигается:

1. Уменьшением значения λ_2, что обеспечивается точностью и скоростью классификации происходящих инцидентов и определения адекватных мер реагирования;

2. Увеличением значения m_6^0, что обеспечивается полнотой классификатора при распознавании событий безопасности;

3. Уменьшением значения λ_6, что достигается повышением результативности реализации мер реагирования на инциденты и мер по восстановлению нормального функционирования процессов.

Таким образом, для решения вышеперечисленных задач необходимо разработать:

1) структуру модели реагирования на инциденты безопасности, обеспечивающую достижение вышеперечисленных целей;

2) метод и алгоритм классификации инцидентов ИБ, позволяющие учесть неточную информацию об инциденте ИБ, представленную не в формализованном виде, а также эффективно работающие в условиях жесткого ограничения времени;

3) методику формирования планов реагирования на инциденты ИБ, которая должна включать процедуры установки требований к операционной устойчивости информационных активов и определения их критичности для функционирования бизнес-процессов.

Кроме того, для обеспечения непрерывного совершенствования системы, которое во многом определяет повышение значения коэффициента m_6^0, должно быть обеспечено накопление знаний о произошедших инцидентах с целью переобучения классификатора и корректировки планов реагирования на инциденты ИБ и, как следствие, повышения скорости реакции, качества классификации инцидентов и выработки более эффективных мер реагирования.

Для решения поставленных задач предложена следующая структура модели ИСУ (интегрированной системы управления) операционной устойчивостью бизнес-процессов в условиях реализации угроз ИБ (рис. 2).

Модуль D1 разработан для обеспечения сбора информации об инциденте безопасности, необходимой и достаточной для корректной классификации инцидента. Результатом работы модуля является набор атрибутов инцидента (например, характер инцидента, степень влияния на бизнес-процессы, затронутые информационные активы).

Полученный на выходе модуля D1 набор атрибутов инцидента служит входом для модуля D2, результатом работы которого является оценка класса инцидента. Классификация инцидента происходит с использованием дерева решений, таким образом, на вход модуля также должно поступать построенное дерево решений. Эту задачу решает модуль Р1, в котором определяются метод формирования правил классификации, алгоритм построения и алгоритм обхода дерева решений. В качестве атрибутов инцидента могут выступать признаки, которые невозможно определить однозначно: если количество затронутых пользователей можно определить точно значениями «20» или «45», то для признака «уровень угрозы репутации» это сделать затруднительно. Таким образом, в модуле Р1 при определении правил классификации используется аппарат теории нечетких множеств.

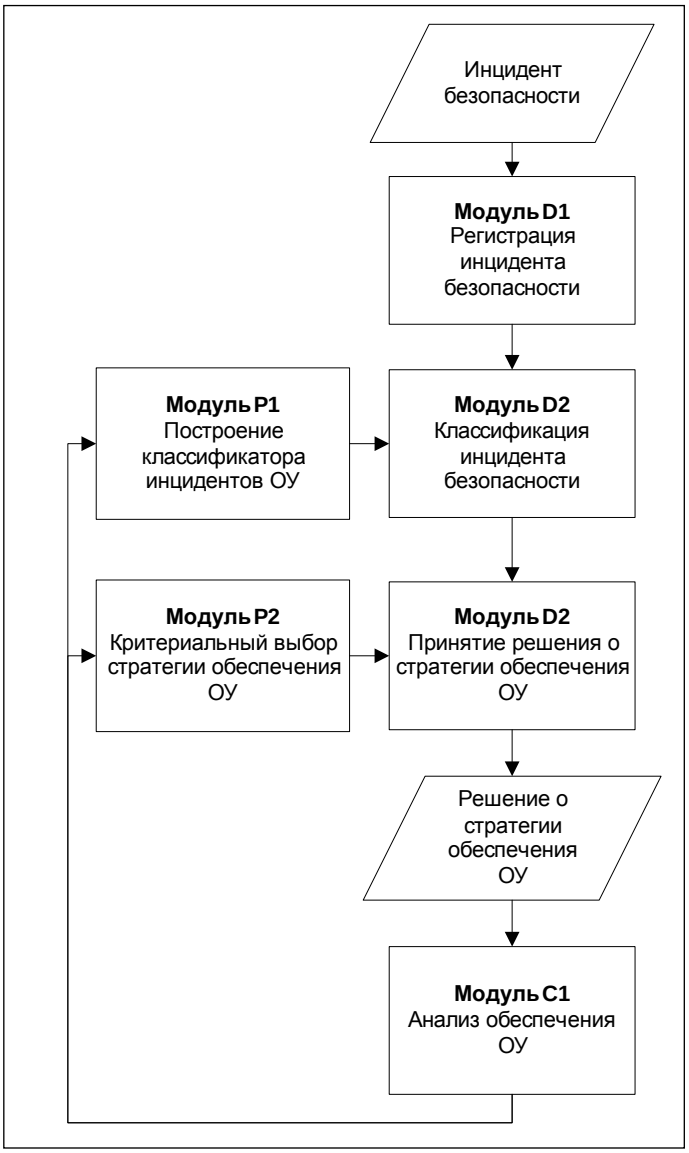

Рис. 2. Структура модели ИСУ

Полученный в модуле D1 класс инцидента служит входом для модуля D3, целью работы которого является формирование решения относительно стратегии обеспечения операционной устойчивости. Данное решение может быть принято только на основе оценки множества альтернатив, что реализуется в модуле P2 на основе критериального подхода. Кроме того, реализация выбранной стратегии управления операционной устойчивостью обеспечивается за счет своевременного формирования планов и процедур, соответствующих определенной стратегии. Эта задача решается группой экспертов, в которую должны входить руководители линейных подразделений, технические специалисты и специалисты по ИБ.

Модуль C1 получает информацию о классификации инцидента, принятых ответных мерах и результатах реализации мер. Проводится сравнение целевых и реальных параметров обеспечения операционной устойчивости. Анализируются точность классификации инцидента, корректность определенных ответных мер, скорость возврата к нормальному функционированию бизнес-процессов. Результаты анализа могут инициировать изменения в модуле P1 в части переобучения дерева решений и в модуле P2 в части внесения корректировок в состав стратегий обеспечения операционной устойчивости и соответствующих им планов и процедур. Результатом

изменений является уменьшение времени реагирования и времени восстановления нормального функционирования процессов при последующих инцидентах, а следовательно, повышение общего уровня операционной устойчивости.

В своей совокупности модули образуют полный цикл Шухарта—Деминга, который лежит в основе большинства стандартов по управлению ИБ [5]: модули P1—P2 относятся к этапу Plan (планирование), модули D1—D3 — к этапу Do (действие), модуль C1 — к этапу Check (оценка), этап Act (воздействие, корректировка) реализуется за счет введенной обратной связи. Таким образом, можно говорить о согласованности предлагаемой модели с существующими практиками.

СПИСОК ЛИТЕРАТУРЫ:

1. Software Engineering Institute. CERT Resilience Management Model. Improving Operational Resilience Processes. Technical report, 2011. — 259 с.
2. *Блюмин С. Л., Шмырин А. М., Седых И. А., Филоненко В. Ю.* Окрестностное моделирование сетей Петри: монография. Липецк: ЛЭГИ, 2010. — 124 с.
3. *Андрианов В. В., Зефиров С. Л.* Обеспечение информационной безопасности бизнеса. М.: ЦИПСиР — Альбина Паблишерз, 2011. — 373 с.
4. ГОСТ Р ИСО/МЭК 18044: 2007. Информационная технология. Методы и средства обеспечения безопасности.
5. *Демин П. А.* Проблемы реализации систем управления информационной безопасностью на основе стандартизированных моделей // Безопасность информационных технологий. 2011. № 1. С. 160—163.