РАЗДЕЛ 6. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК: 004.023: 004.041

РАСЧЕТ ОЦЕНКИ ПРЕДСКАЗАНИЯ ОТ УЩЕРБА В ЗАВИСИМОСТИ ОТ РЕАЛИЗАЦИИ НЕБЛАГОПРИЯТНЫХ СОБЫТИЙ В КОМПЬЮТЕРНОЙ СИСТЕМЕ С ПОМОЩЬЮ МОДЕЛИ В ФОРМЕ ПРОСТРАНСТВА СОСТОЯНИЙ

А.Ж. Абденов, Р.Н. Заркумова-Райхель

В работе предложена методика расчета оценки предсказания от ущерба, нанесенного информационным ресурсам в компьютерной системе предприятия, от реализации неблагоприятных событий. Оценки предсказания рассчитываются на основе дискретных уравнений фильтра Калмана.

Ключевые слова: ущерб, информационные ресурсы, неблагоприятные события, модель в пространстве состояний, фильтр Калмана.

Введение

Основанный на рисках подход к оценке предсказания потенциального ущерба от атак нарушителей и выбору мер для его минимизации получил название управления рисками. Под управлением рисками подразумевается полный комплекс из ряда выполняемых последовательно процессов, что соответствует существующим международным стандартам и практике управления рисками в организациях [1]: определение контекста, идентификация рисков, анализ рисков, принятие рисков, мониторинг и пересмотр.

Под анализом риска понимаются данные, полученные после обработки результатов наблюдений. Результаты работы системного аналитика используются лицами, принимающими решения [2, 3]. Модели анализа и оценки рисков исторически прошли три стадии развития [3, 4]. В первых моделях использовались эвристические оценки всех возможных угроз. В моделях второй стадии риски в области информационных технологий рассматриваются как случаи: общего риска деловой деятельности, когда оценка рисков исходит из стоимостной оценки информационных ресурсов. Третье поколение моделей рассматривает управление рисками как принятие решений в условиях неопределенности, а количественные показатели риска - как критерии принятия альтернативных или взаимодополняющих решений в процессе какой-либо деятельности. Неопределенность, учитываемая в моделях третьего поколения, объясняется недостаточными субъективными знаниями о предмете или ситуации (субъективная вероятность), в отличие от объективной вероятности (полученной на основе статистики, накопленной на предприятии, или в мире для аналогичных условий и аналогичных инцидентов) , которая является мерой возможности реализации неблагоприятных событий (НС) в информационной системе, приводящей к ущербу [4, 5].

Указанные подходы имеют непосредственное приложение к решению задач обеспечения безопасности информационных ресурсов, а количественные показатели рисков в такого рода задачах становятся количественными показателями безопасности информационных ресурсов (ИР). Как отмечалось выше, риск является одним из основополагающих понятий системного анализа. Следуя подходу Кумамото и Хенли [5], а также идеям, отраженных в работе [4], примем более узкое практическое направление формального определения параметров, характеризующих риски нарушения безопасности информационных ресурсов. Во-первых, необходимо классифицировать виды атак нарушения безопасности информационных ресурсов. Заметим, что в настоящее время для снижения уровня риска и защиты от угроз на предприятиях применяются различные контроли [6]. При этом реализация одних видов контролей может повлиять на выбор и реализацию контролей других видов. Во-вторых, для описания статистических данных наблюдений, накопленных относительно каждого вида атак O_i, которые характеризуют количество нарушений каждого вида атак и стоимостную оценку ущерба от нарушений безопасности ИР, будем использовать два параметра:

- объективную вероятность, рассчитываемую через накопленную статистику о фактах нарушений безопасности ИР, которую обозначим через $\{P(O_i),\ i=\overline{1,m}\}$ - где i - индекс, характеризующий вид атаки; m - общее количество видов атак;
- объективную стоимостную оценку ущерба $\{S_i(O_i),\ i=\overline{1,m}\}$ безопасности ИР.

Методическая оценка ущерба в информационной системе (ИС) от реализации неблагоприятных событий (НС) существенно зависит от оценки риска. Оценки риска рассчитываются в зависимости от вероятности реализации НС в ИС. Различают объективные и субъективные вероятности в возможности наступления НС. Рассмотрим теперь один из возможных подходов к расчету объективной вероятности неблагоприятных событий на основе независимой статистики, которая имеется на предприятии.

Расчет объективной вероятности

Пусть общий список НС представляет собой множество видов НС $\{O_1, O_2, \ldots, O_m\}$, возникающих в ИС и приводящих к снижению системной эффективности компьютерной системы (КС). Выделим из этого множества некоторое существенное подмножество некоторых видов НС, приводящих к ощутимому нарушению безопасности информационных ресурсов (ИР) в КС. Это подмножество обозначим через

$$O=\{O_{i_1}, O_{i_2}, \ldots, O_{i_m}\} \le \{O_1, O_2, \ldots, O_m\}.$$

Например, O_{i_1} - количество НС относительно нарушения запуска отдельных узлов КС; O_{i_2} - количество НС относительно неверного набора информации применительно к конкретному информационному процессу и обработке данных и т.д.

После построения подмножества O переходим к анализу свойств элементов подмножества на основе количественных показателей НС и величины ущерба, имевших место в прошлом. Пусть математическое ожидание ущерба, вызываемого i - м НС за время ΔT (например, 1 месяц), выражается формулой:

$$e(O_i, \Delta T) = M[e(O_i)\cdot f_i], i=\overline{1,m}, \quad (1)$$

где $e(O_i)$ - случайная величина ущерба уже случившегося НС при единичном наступлении НС; f_i - случайная величина количества НС за время ΔT; m - общее количест-во всех видов НС уже свершившихся НС.

Если НС не имеют последствия в том смысле, что ущерб от каждого НС независим, то

$$e(O_i, \Delta T) = M[e(O_i)]\cdot M[f_i], i=\overline{1,m}, \quad (2)$$

$$E(O, \Delta T) = \sum_{i=1}^{m} M[e(O_i)]\cdot M[f_i]. \quad (3)$$

Для простоты будем рассматривать лишь один вид НС. Зафиксируем конкретное значение i =1.Далее, сведем количественные помесячные показатели НС, например, за 3 года в следующую таблицу 1.

Таблица 1. Количественные показатели произошедших НС в течение последних лет по месяцам

i	1	2	3	4	5	6	7	8	9	10	11	12
2008	$f_1^{(1)}$	$f_2^{(1)}$	$f_3^{(1)}$	$f_4^{(1)}$	$f_5^{(1)}$	$f_6^{(1)}$	$f_7^{(1)}$	$f_8^{(1)}$	$f_9^{(1)}$	$f_{10}^{(1)}$	$f_{11}^{(1)}$	$f_{12}^{(1)}$
2009	$f_1^{(2)}$	$f_2^{(2)}$	$f_3^{(2)}$	$f_4^{(2)}$	$f_5^{(2)}$	$f_6^{(2)}$	$f_7^{(2)}$	$f_8^{(2)}$	$f_9^{(2)}$	$f_{10}^{(2)}$	$f_{11}^{(2)}$	$f_{12}^{(2)}$
2010	$f_1^{(3)}$	$f_2^{(3)}$	$f_3^{(3)}$	$f_4^{(3)}$	$f_5^{(3)}$	$f_6^{(3)}$	$f_7^{(3)}$	$f_8^{(3)}$	$f_9^{(3)}$	$f_{10}^{(3)}$	$f_{11}^{(3)}$	$f_{12}^{(3)}$

Исходя из данных таблицы 1, с помощью следующей формулы (4), можно получить одну строку данных усредненных значений по столбцам (таблица 2):

$$f_j = \sum_{i=1}^{3} f_j^{(i)}/3,\ \ j=\overline{1,12}. \quad (4)$$

Таблица 2. Усредненная строка количественных показателей произошедших НС в течение 2008, 2009, 2010 гг. по месяцам

i	1	2	3	4	5	6	7	8	9	10	11	12
$f_i^{уср}$	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}

Аналогичные таблицы необходимо построить относительно других видов НС усредненных количественных случайных величин ущерба уже соответствующих случившихся НС при каждом единичном наступлении НС.

Применительно к усредненным данным таблицы 2, можно построить математическую модель в форме пространства состояний (по методике, изложенной в [7]) вида:

$$x(t+1) = a_i\cdot x(t) + b_i\cdot u(t) + w(t),$$
$$x(0) = x_0, \quad (5)$$

$$f^{ycp}(t+1) = x(t+1) + v(t+1),$$
$$t = \overline{0, N-1},\ i = 1, 2, 3. \quad (6)$$

где $x(t)$ - количество НС в момент времени t; $u(t)$ - внешнее управляющее воздействие на анализируемый вид НС в момент времени t; $w(t)$ - случайное ненаблюдаемое воздействие в момент времени t; x_0 - количество НС в начальный в момент времени $t = 0$; a_i, b_i - неизвестные коэффициенты в модели динамики (5); t - номер месяца в году; $N = 12$ - число месяцев в году;

$f^{ycp}(t)$ - наблюдаемое случайное количество НС к моменту времени t (данные из журнала наблюдений предприятия); $v(t)$ - случайная величина ошибок наблюдений относительно количества НС в течении месяца.

Будем предполагать, что шумы динамики $w(t)$, измерительной системы $v(t)$ – есть белые гауссовские последовательности с дисперсиями Q, R соответственно, а шум начального состояния x_0 - есть гауссовская величина с математическим ожиданием и дисперсией $P(0)$. Далее необходимо оценить все характеристики, связанные с шумами измерительной системы, шумами относительно модели динамики и шумом величины начального состояния по формулам, которые изложены в работах [7,8]: Это позволит получить оценки $\hat{Q}$, $\hat{R}$, $\hat{P}(0)$.

Построенная модель (5), (6) позволит, с помощью уравнений фильтра Калмана, получить наиболее достоверные оценки количества НС в режиме реального времени, относительно каждого месяца в виде оценок фильтрации [7] за последующий, например, 2011 г. Оценки фильтрации позволят рассчитать объективные вероятностные оценки реализаций НС. Предлагается следующая методика расчета вероятности для конкретного вида НС. Пусть нас интересует вероятность появления НС в каждом месяце предыдущего i-года. Для этого подсчитывается общее суммарное ко-личество НС в течение всего i-года ($F^{(i)}$), а затем фильтрационная оценка количества НС в течение каждого месяца ($f^{(i)}(t)$) делится на общее суммарное фильтрационное количество НС в течении одного i-того года по формуле:

$$p^{(i)}(t) = f^{(i)}(t) / F^{(i)}, \quad t = \overline{1, 12}, i = 4, \quad (7)$$

где $p^{(i)}(j) = p_j^{(4)}$ - объективная вероятность реализации конкретного вида НС в течение каждого месяца i-того года (например, i=4) и всех 12 месяцев будет иметь вид таблицы 3.

Таблица 3. Значения объективной вероятности реализаций конкретного вида НС по месяцам в течение одного года (i=4)

t	1	2	3	4	5	6	7	8	9	10	11	12
2011	$p_1^{(4)}$	$p_2^{(4)}$	$p_3^{(4)}$	$p_4^{(4)}$	$p_5^{(4)}$	$p_6^{(4)}$	$p_7^{(4)}$	$p_8^{(4)}$	$p_9^{(4)}$	$p_{10}^{(4)}$	$p_{11}^{(4)}$	$p_{12}^{(4)}$

При этом для i=4 будем иметь:

$$\sum_{j=1}^{12} p^{(i)}(j) = 1, \quad i = 4, 5, \ldots. \quad (8)$$

Объективная стоимостная оценка ущерба

Пусть $O = \{O_i, i = \overline{1, m}\}$ - множество видов неблагоприятных событий, приводящих к нарушению безопасности информационных ресурсов. Выше была предложена методика расчета помесячной объективной вероятности количества нарушений определенного вида атаки на информационные ресурсы в ИС условного предприятия. Предположим, что в отделе информационной безопасности предприятия имеется статистика относительно ежемесячной оценки ущерба, которая соответствует ежемесячному количеству нарушений информационной безопасности конкретного i- того вида атаки, т.е. таблице 1 соответствует таблица 4.

Таблица 4. Количественные ежемесячные показатели ущерба, от нарушений информационной безопасности в зависимости от i- го вида атаки

i	1	2	3	4	5	6	7	8	9	10	11	12
2008	$S_1^{(1)}$	$S_2^{(1)}$	$S_3^{(1)}$	$S_4^{(1)}$	$S_5^{(1)}$	$S_6^{(1)}$	$S_7^{(1)}$	$S_{18}^{(1)}$	$S_9^{(1)}$	$S_{10}^{(1)}$	$S_{11}^{(1)}$	$S_{12}^{(1)}$
2009	$S_1^{(2)}$	$S_2^{(2)}$	$S_3^{(2)}$	$S_4^{(2)}$	$S_5^{(2)}$	$S_6^{(2)}$	$S_7^{(2)}$	$S_{18}^{(2)}$	$S_9^{(2)}$	$S_{10}^{(2)}$	$S_{11}^{(2)}$	$S_{12}^{(2)}$
2010	$S_1^{(3)}$	$S_2^{(3)}$	$S_3^{(3)}$	$S_4^{(3)}$	$S_5^{(3)}$	$S_6^{(3)}$	$S_7^{(3)}$	$S_{18}^{(3)}$	$S_9^{(3)}$	$S_{10}^{(3)}$	$S_{11}^{(3)}$	$S_{12}^{(3)}$

Заметим, что не всегда ежемесячные показатели ущерба прямо пропорциональны количеству произошедших НС. Поэтому по данным таблицы 4 необходимо построить линейную модель в форме пространства состояний (ПС), которая будет соответствовать усредненным по столбцам данным таблицы 4 вида таблицы 5, данные которой вычисляются с помощью соотношения (9)

Таблица 5. Усредненная строка ежемесячных количественных показателей ущерба, нанесенного ИР предприятия

k	1	2	3	4	5	6	7	8	9	10	11	12
$s_k^{(y)}$	$s_1^{(y)}$	$s_2^{(y)}$	$s_3^{(y)}$	$s_4^{(y)}$	$s_5^{(y)}$	$s_6^{(y)}$	$s_7^{(y)}$	$s_8^{(y)}$	$s_9^{(y)}$	$s_{10}^{(y)}$	$s_{11}^{(y)}$	$s_{12}^{(y)}$

На основе строки данных $\left\{s_k^{(y)},\ k=\overline{1,12}\right\}$ по алгоритмам описанных в работах [7, 8] можно построить линейную модель в форме пространства состояний вида

$$s(t+1)=\hat{c}\cdot s(t)+\hat{d}\cdot+w(t),\ t=\overline{0,11},$$
$$s(0)=s_0, \qquad (10)$$
$$s^y(t+1)=s(t+1)+v(t+1).$$

Предположим, что мы располагаем данными наблюдений количественных показателей ущерба нанесенных на ИР предприятия в 2011 году вида таблицы 6.

Таблица 6. Ежемесячные количественные показатели ущерба, нанесенных информационным ресурсам предприятия в 2011 году

k	1	2	3	4	5	6	7	8	9	10	11	12
$\hat{s}(t\mid t)$	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}

Используя уравнения фильтра Калмана и данные таблицы 6, получим последовательность оценок фильтрации $\left\{\hat{s}(t\mid t),\ t=\overline{1,12}\right\}$,относительно ежемесячных количественных показателей ущерба нанесенных ИР предприятия.

Теперь, используя данные таблицы 3, относительно количественных показателей свершившихся НС в течение 2011 года по месяцам и данных таблицы 6 относительно количественных показателей ущерба нанесенных на ИР предприятия в 2011 году можно получить усредненный ущерб нанесенных от единич-ного случая свершившегося НС $\left\{e(t),\ t=\overline{1,12}\right\}$.

Расчетные данные можно свести в таблицу 7.

Таблица 7. Усредненный ущерб нанесенных от единичного случая свершившегося НС

t	1	2	3	4	5	6	7	8	9	10	11	12
e(t)	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}

Далее, используя данные оценок предсказания относительно количества НС на будущий месяц, полученные по модели (5), (6) в режиме реального времени и умножая на соответствующее усредненное значение объективной стоимости ущерба на одну единицу НС из таблицы 7, мы получим объективную стоимость оценки предсказания ущерба на предстоящий месяц.

Заключение

Управление рисками базируется на данных, которые должны фиксироваться, накапливаться, анализироваться, храниться, обрабатываться для целей оценивания потенциального ущерба от ошибок пользователей и атак нарушителей на ИР в ИС предприятия, выбора мер для его минимизации, расчета оценок предсказания всех возможных параметров и показателей, связанных с информационной безопасностью. В данной работе, в частности, были предложены методики, позволяющие получать оценки объективной вероятности наступлений НС, оценки объективной стоимости ущерба от нарушений безопасности ИР в ИС предприятия и помесячные оценки предска-зания величины ущерба. Все основные расчеты показателей информационной безопасности ИР предприятия могут использовать возможности линейной стохастической модели в форме пространства состояний и уравнений фильтра Калмана для получения более достоверных значений оценок состояния исследуемого объекта в режиме реального времени.

$$S_k^{(y)}=\sum_{i=1}^{3}S_k^{(i)},\ k=\overline{1,12}. \qquad (9)$$

СПИСОК ЛИТЕРАТУРЫ

1. ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management. 2008.
2. Vose, D. Risk analysis: a quantitative guide./ D.Vose.- 3-rd edition. John Wiley&Sons, 2008.
3. SooHoo, K. How much is enough? A risk – management approach to computer security [электронный ресурс]. Phd thesis. Stanford University, 2001.Режим доступа: http:// iis-db.stanford.edu/pubs/11900/soohoo.pdf.
4. Запечников, С.В. Модель методической оценки возможного ущерба в информационной системе от реализации неблагоприятных событий/ С.В. Запечников // Информационная безопасность, № 3. 2010.С. 10-14.

5. Kumamoto H., Henley E. Probabilistic risk assessment and management for engineers and scientists/ H.Kumamoto,E. Henley//2-nd edition. Institute of Electrical and Electronics Engineers. Inc. New York, 1996.
6. Chi-Chun Lo, Wan-Jia Chen. A hyd information security risk assessment procedure considering interdependences between controls // Expert Systems with Applications. 2011. V. 39. P. 248-257.
7. Заркумова-Райхель, Р.Н. Прогнозирование количества инцидентов в системе информационной безопасности предприятия при помощи динамической модели /Р. Н. Заркумова-Райхель, А.Ж. Абденов// Фундаментальные исследова-ния, No.6 (2). 2012.С. 429-434.
8. Абденова, Г.А. Прогнозирование значений уровня временного ряда на основе уравнений фильтра Калмана/Г.А. Абденова. // Ползуновский вестник. Барнаул: АлтГТУ, 2010. № 2. С. 4–6.

Профессор кафедры защита информации, ***Абденов А.Ж,.*** *д.т.н., профессор, тел. 8-923-151-77-21 amirlan21@gmail.ru; соискатель кафедры защита информации* ***Заркумова-Райхель Р.Н.*** *zarkumova@gmail.com - Новосибирский государственный технический университет.*

УДК: 519.24

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ НЕИНТЕРАКТИВНЫХ АНАЛОГОВ Σ-ПРОТОКОЛОВ С БИНАРНЫМИ ЗАПРОСАМИ

А.Б. Фролов

В статье рассматриваются неинтерактивные аналоги протоколов идентификации (Σ-протоколов) с бинарными запросами. Показано, что для повышения их устойчивости число проверок может быть увеличено при сохранении информационной скорости за счет применения эффективной забывающей передачи при многократном использовании единого рандомизатора.

Ключевые слова: протокол с нулевым разглашением секрета, протокол идентификации, бинарный запрос, забывающая передача, рандомизатор, информационная скорость.

Введение

Интерактивные и неинтерактивные протоколы с нулевым разглашением секрета являются весьма важными криптографическими примитивами современных криптосистем таких как электронные платежные системы, электронные системы голосования, сохраняющие приватность интеллектуальные измерительные системы и др. [1]. Они обеспечивают идентификацию участников протокола. Протокол доказательства с нулевым разглашением $(P,V)(x)$ исполняется двумя участниками — доказывающим P и проверяющим V, владеющими общей информацией x [2]. Эта общая информация может быть значением $z=f(s)$ односторонней функции $f(s)$, прообраз s которого является секретом P. Исполняя протокол, P убеждает проверяющего V, что он владеет секретом s, не разглашая никакой информации о секрете. Такие протоколы имеют две вероятностные характеристики: *полнота* σ (нижняя граница вероятности успешного доказательства честным доказывающим P и *неустойчивость* δ (верхняя граница вероятности успешного доказательства нечестным доказывающим $\widetilde{P}$, не владеющим секретом, — граница неустойчивости). Понижение этого порога означает повышение устойчивости протокола. В этой статье мы рассматриваем протоколы, для которых $\sigma=1$, $\delta\le 1/2$. Третьей характеристикой является *совершенство* — полное скрытие секрета в процессе исполнения протокола. Информационная скорость зависит от длины транзакции, пересылаемой от P проверяющему, она тем больше, чем короче транзакция.

Имеются два типа протоколов с нулевым разглашением секрета: интерактивные и неинтерактивные. Интерактивный протокол (т.н. Σ-протокол) обычно исполняется в три раунда [3]:

1) Сообщение *commit*, являющееся значением c односторонней функции, соответствующим текущему случайно выбранному секретному значению *committal*, пересылается доказывающим P проверяющему V.

2) Сообщение *challenger*, являющееся случайно выбранной бинарной строкой e длины t, $t \ge 1$, пересылается от V к P.

3) Сообщение r *response*, зависящее от *committal*, *challenger* и от секрета s пересылается от P к V. (s скрывается случайным сообщением *committal*).

После этих обменов V проверяет ответ *response* по значению предиката *Verify*(c,e,r,z). Если это значение *true*, то принимает доказательство, иначе отклоняет. При t=1 мы называем такие протоколы Σ-протоколами с бинарными запросами, при t>1 — Σ-протоколами с множественными запро-