УПРАВЛЕНИЕ В СОЦИАЛЬНЫХ И ЭКОНОМИЧЕСКИХ СИСТЕМАХ

УДК 004.056

И. М. Ажмухамедов, О. М. Князева

УНИФИКАЦИЯ ПОДХОДОВ К УПРАВЛЕНИЮ УРОВНЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ РАЗЛИЧНОГО ПРОФИЛЯ

Разработана унифицированная методика управления уровнем информационной безопасности, которая включает в себя два этапа: оценку текущего уровня информационной безопасности на основе нечетких продукционных правил и синтез управляющих решений на основе применения нечеткого когнитивного моделирования для вывода сервисов информационной безопасности на необходимый целевой уровень. Алгоритм оценки уровня информационной безопасности представлен в виде итерационного процесса, включающего в себя следующие этапы: вербальная оценка уровня повреждений; поиск соответствующих правил в базе знаний; оценка состояния сервисов безопасности на текущем уровне иерархии согласно найденным правилам; идентификация и исключение из рассмотрения блоков, содержащих повреждения, уровень которых не позволяет идентифицировать повреждения некоторых блоков на следующем уровне; вычисление интегральной оценки сервисов безопасности и обобщенного показателя информационной безопасности объекта информатизации в целом. Методика оценки уровня информационной безопасности не предусматривает решение задачи выработки управляющих решений для вывода сервисов информационной безопасности на необходимый целевой уровень, поскольку в ней не содержится информация о причинно-следственных связях между наблюдаемыми повреждениями информационных активов и средств защиты информации и угрозами и уязвимостями, сделавшими возможной реализацию атак, которые привели к наблюдаемым повреждениям. Для решения задачи второго этапа была построена модель, отражающая связи между повреждениями информационных активов и средств защиты информации, угрозами и уязвимостями. Оценка уровня информационной безопасности на основе нечетких продукционных правил дает возможность лицу, принимающему решения, вырабатывать обоснованное суждение о необходимости синтеза управляющих решений для вывода сервисов безопасности на заданный целевой уровень, а нечеткая когнитивная модель позволяет синтезировать данные управляющие решения. Методика управления уровнем информационной безопасности была апробирована в ряде организаций. Результаты апробации позволили сделать вывод о возможности использования методики в организациях различного профиля деятельности.

Ключевые слова: информационная безопасность, сервисы безопасности, угрозы, уязвимости, повреждения, меры защиты, лингвистическая переменная, нечеткие числа.

Введение

Существенное влияние на процесс обеспечения информационной безопасности организации оказывает профиль ее деятельности. Это связано с тем, что он определяет:

- виды информации, с которой работает организация (коммерческая тайна, профессиональная тайна, служебная тайна, персональные данные и т. д.);
- способы обработки информации и каналы ее передачи;
- уровень доступа посторонних лиц на территорию организации и т. д.

Отметим, что каждая организация вынуждена искать свои методы и способы управления уровнем информационной безопасности. Унификация подходов позволила бы снизить трудоемкость данного процесса.

Постановка задачи

С учетом вышесказанного была определена задача исследований – разработка унифицированной методики управления уровнем информационной безопасности (ИБ).

Методика управления уровнем информационной безопасности

Управление уровнем ИБ является итерационным процессом и включает в себя два этапа:

– оценка текущего уровня ИБ (сервисов «Конфиденциальность», «Целостность», «Доступность»);

– синтез управляющих решений для вывода сервисов ИБ на необходимый целевой уровень.

Рассмотрим решение задач каждого этапа более подробно.

Оценка текущего уровня информационной безопасности. В основе предлагаемого нами подхода к оценке текущего уровня ИБ лежит применение нечетких продукционных правил (НПП).

Будем считать, что состояние сервисов ИБ характеризуется интенсивностью повреждений информационных активов (ИА) и средств защиты информации (СЗИ). Отметим, что под повреждением имеется в виду нарушение нормального (соответствующего требованиям ИБ) режима функционирования, а под ИА, согласно ГОСТ Р ИСО/ТО 13569-2007, понимаются информационные ресурсы и средства обработки информации.

Уровень повреждений обычно определяется лицом, принимающим решение (ЛПР), на основании наблюдений и формулируется им в виде лингвистических оценок. Для формализации таких оценок введем лингвистическую переменную «Уровень фактора» и терм-множество ее значений *QL*, состоящее из 5 элементов:

$$QL = \{\text{Низкий } (\text{Н}),\ \text{Ниже среднего } (\text{НС}),$$

$$\text{Средний } (\text{С}),\ \text{Выше среднего } (\text{ВС}),\ \text{Высокий } (\text{В})\}.$$

В качестве семейства функций принадлежности для *QL* будем использовать пятиуровневый классификатор, в котором функциями принадлежности нечетких чисел, заданных на отрезке [0, 1] □ *R*, являются трапеции

$$\{XX(a_1, a_2, a_3, a_4)\},$$

где a_1 и a_4 – абсциссы нижнего, a_2 и a_3 – абсциссы верхнего основания трапеции.

Суть данного нечеткого классификатора в том, что если о факторе неизвестно ничего, кроме того, что он может принимать любые значения в пределах 01-носителя (принцип равнопредпочтительности), а надо провести ассоциацию между качественной и количественной оценками фактора, то предложенный классификатор делает это с максимальной достоверностью [1].

Для формализации экспертных суждений, отражающих влияние наблюдаемых повреждений ИА и СЗИ на уровень сервисов безопасности, используем набор НПП, которые образуют базу знаний (БЗ), вида

$$\text{Если}\left(\&_{i=1}^{N}\left[Des_i = D_i\right]\right)\text{То}\left(\&_{j=1}^{3}\left[\left(O_j\right)\left(K_j = S_j\right)\right]\right),$$

где D_i, $S_j \in QL$ – лингвистические оценки уровня повреждения ИА и СЗИ и оценки состояния сервисов безопасности соответственно; символ «=» используется в качестве оператора сравнения; условия $Des_i = D_i$ определяют уровень i-го повреждения ИА или СЗИ; выводы $K_j = S_j$ определяют состояние j-го сервиса безопасности; O_j отражает степень уверенности эксперта в выводе и, согласно шкале Харрингтона, имеет следующие вербальные интерпретации: 0,00–0,20 – невозможно; 0,20–0,37 – маловероятно; 0,37–0,63 – возможно; 0,63–0,80 – весьма возможно; 0,80–1,0 – точно.

С целью учета ситуации при формировании БЗ, когда при высоком уровне одних повреждений невозможно определить уровень других, была построена иерархия повреждений, состоящая из 4 уровней и включающая в себя 13 блоков (рис.). Отметим, что внутри одного уровня иерархии повреждения не влияют друг на друга; повреждения, находящиеся на более низких уровнях иерархии, при определенных условиях могут влиять на возможность идентификации повреждений более высоких уровней.

Иерархию повреждений можно легко адаптировать к специфическим особенностям организаций путем изменения блоков, входящих в иерархию повреждений; связей между блоками; наборов критических повреждений и т. д.

Для заполнения БЗ предлагается использовать следующий алгоритм:

1. Эксперты определяют «атомарные» правила вида

$$\text{Если}\left[Des_i = D_i\right]\text{То}\left[\left(O_i\right)\left(K_j = S_i\right)\right]. \quad (1)$$

Данные правила отражают влияние каждого уровня повреждения элементов в блоках иерархии на сервисы безопасности. Общее количество атомарных правил при этом составляет 295.

2. Для оценки влияния повреждений *k*-го блока, наблюдаемых ЛПР, в целом на *j*-й сервис безопасности K_j^k , воспользуемся *«блоковыми»* правилами вида

$$K_j^k:\text{Если}\left(\&_{i=1}^{W}\left[Des_i = \overline{D_i}\right]\right)\text{То}\left(\&_{j=1}^{M}\left[\max_m\{O_m\}_{m\in\{\arg(\min_i(\overline{S_i}))\}}\left(K_j^k = \min_i\left(\overline{S_i}\right)\right)\right]\right),$$

где W – количество повреждений в *k*-м блоке; $\overline{D_i}$ – уровень наблюдаемых повреждений Des_i; M – количество сервисов безопасности, на которые влияют повреждения *k*-го блока; $\overline{S_i}$ – определяемое согласно соответствующему атомарному правилу значение сервиса безопасности K_j при уровне повреждения Des_i , равном $\overline{D_i}$; O_m – степень уверенности эксперта в оценке влияния повреждения Des_i, имеющего уровень $\overline{D_i}$, на *j*-й сервис безопасности.

Полученная таким образом совокупность «*блоковых*» правил и образует БЗ.

При этом БЗ является полной, поскольку для каждого набора уязвимостей определен логический вывод; неизбыточной, поскольку ликвидация хотя бы одного правила делает БЗ неполной; непротиворечивой, поскольку исключена ситуация, когда два и более правил БЗ имеют одинаковые левые и разные правые части.

Важным этапом создания БЗ является определение множества *«узловых»* повреждений блоков и их «*критических*» уровней. Под *«узловыми»* понимаются повреждения, которые при достижении определенного («*критического*») уровня не позволяют идентифицировать повреждения некоторых блоков на следующем уровне.

Определение «*критических*» уровней «*узловых*» повреждений блоков на каждом уровне иерархии осуществляется экспертами.

Для составления БЗ в качестве экспертов были привлечены представители правоохранительных и контролирующих органов государственной власти, а также преподаватели профильных кафедр Астраханского государственного технического университета (АГТУ).

Иерархия повреждений: ПО – программное обеспечение;
НСД – несанкционированный доступ

Получение экспертных данных осуществлялось методом комиссии. Каждому эксперту предоставлялся список атомарных правил вида (1) с заполненными левыми и пустыми правыми частями:

Если [Повреждения каналов передачи данных = Н] То [(_____) (Сервис «Доступность» (сД) = _____)];

Если [Повреждения каналов передачи данных = Н] То [(_____) (Сервис «Целостность» (сЦ) = _____)];

Если [Повреждения каналов передачи данных = НС] То [(_____) (Сервис «Доступность» (сД) = _____)];

Если [Повреждения файлов на рабочих станциях = В] То [(_____) (Сервис «Доступность» (сД) = _____)];

Если [Повреждения файлов на рабочих станциях = В] То [(_____) (Сервис «Целостность» (сЦ) = _____)].

Эксперту необходимо было оценить (с определенной степенью уверенности) влияние каждого повреждения (левая часть правила) на сервисы безопасности (правая часть правила).

Итоговые значения уровней сервисов безопасности были определены коллективно – путем проведения экспертами открытой дискуссии.

Эксперты определили также «*критические*» значения «*узловых*» повреждений блоков на каждом уровне иерархии:

– для элементов блока физических повреждений серверов ИС «*критическое*» значение оказалось равным ВС;
– для элементов блока физических повреждений рабочих станций ИС – ВС;
– для повреждений системного ПО серверов – С;
– для повреждений системного ПО рабочих станций – С;
– для повреждений пользовательского ПО серверов – ВС;
– для повреждений пользовательского ПО рабочих станций – ВС.

На основании изложенного алгоритм оценки уровня ИБ может быть представлен в виде итерационного процесса, включающего в себя следующие этапы: вербальная оценка уровня повреждений; поиск соответствующих правил в БЗ; оценка состояния сервисов безопасности на текущем уровне иерархии согласно найденным правилам; идентификация и исключение из рассмотрения блоков, содержащих «*узловые*» повреждения, уровень которых выше критического; вычисление интегральной оценки сервисов безопасности и обобщенного показателя ИБ объекта информатизации в целом.

Оценка состояния сервисов безопасности на каждом уровне иерархии определяется как минимум значений, полученных в результате применения «*блоковых*» правил рассматриваемого уровня:

$$K_j^l : \max_m \{O_m\}_{m \in \{\arg(\min_k(K_j^k))\}} \left[K_j^l = \min_k \left(K_j^k \right) \right], \quad (2)$$

где K_j^l – j-й сервис безопасности на l-м уровне.

Интегральная оценка сервисов безопасности K_j находится как минимум значений критериев ИБ, найденных на каждом из уровней иерархии повреждений, которые удалось идентифицировать:

$$K_j : \max_m \{O_m\}_{m \in \{\arg(\min_k(K_j^l))\}} \left[K_j = \min_l \left(K_j^l \right) \right].$$

Для нахождения обобщенного показателя ИБ объекта информатизации в целом предлагается использовать мультипликативную свертку интегральных оценок сервисов безопасности:

$$K_0 = \prod_{i=1}^{3} (K_j)^{1/3},$$

где K_0 – обобщенный показатель ИБ объекта информатизации в целом.

Применение мультипликативной свертки обусловлено тем, что она, в отличие от аддитивной, более чувствительна к критериям, имеющим низкие значения.

Синтез управляющих решений. Предложенная методика оценки уровня ИБ не предусматривает решение задачи выработки управляющих решений для вывода сервисов ИБ на необ-

ходимый целевой уровень, поскольку в ней не содержится информация о причинно-следственных связях между наблюдаемыми повреждениями ИА и СЗИ и угрозами и уязвимостями, сделавшими возможной реализацию атак, которые, в свою очередь, привели к наблюдаемым повреждениям.

Таким образом, для решения задачи второго этапа необходима модель, отражающая связи между повреждениями ИА и СЗИ, угрозами и уязвимостями.

При построении такой модели необходимо иметь в виду, что процесс обеспечения ИБ характеризуется рядом особенностей (неполнота и неопределенность исходной информации о составе и характере угроз; невозможность количественного измерения большинства параметров процесса; большое число частных показателей и т. д.). Учесть указанные особенности позволяет нечеткое когнитивное моделирование, неоспоримыми достоинствами которого являются возможность формализации численно неизмеримых факторов и возможность использования неполной, нечеткой и даже противоречивой информации [2–4]. В качестве нечеткой когнитивной модели процесса обеспечения ИБ предлагается принять кортеж [1, 5]:

$$IS = <G, QL, S, R, \Omega>,$$

где G – ориентированный граф, не содержащий горизонтальных ребер в пределах одного уровня иерархии; QL – набор качественных оценок уровней каждого фактора в графе; S – множество весов ребер графа G, отражающих степень влияния концептов на заданный элемент следующего уровня иерархии; R – набор правил для вычисления значений концептов на каждом из уровней иерархии G; Ω – индекс схожести, характеризующий степень соответствия значения фактора той или иной качественной оценке из терм-множества лингвистической переменной QL.

Индекс схожести Ω двух нечетких чисел: $A(a_1, a_2, a_3, a_4)$ и $B(b_1, b_2, b_3, b_4)$ с соответствующими функциями принадлежности $\mu_A(x)$ и $\mu_B(x)$ находим по следующим формулам [1]:

$$\Omega = \frac{\left(1 + \tilde{\rho}\right)}{2},$$

$$\tilde{\rho} = \frac{\rho_{in} - \rho_{out}}{\rho_{in} + \rho_{out}},$$

где

$$\rho_{in} = \int_{a_1}^{a_4} \min\left[\mu_A(x);\ \mu_B(x)\right] dx;$$

$$\rho_{out} = \left| \int_{b_1}^{b_4} \left[\mu_B(x)\right] dx - \rho_{in} \right|.$$

Здесь ρ_{out} – площадь нечеткого числа B (b_1, b_2, b_3, b_4), характеризующего результат, лежащая вне эталонного нечеткого числа $A(a_1, a_2, a_3, a_4)$, а ρ_{in} – площадь, лежащая внутри этого же нечеткого числа).

Вершины графа G на нижнем, пятом, уровне отражают механизмы и СЗИ $P_{\{1, 2, 3, \ldots\}}$. Четвертый уровень представлен угрозами ИБ $UG_{\{1, 2, 3, \ldots\}}$ и уязвимостями $UZ_{\{1, 2, 3, \ldots\}}$.

На 3-м уровне расположены концепты, соответствующие атакам на ИС – $A_{\{1, 2, 3, \ldots\}}$.

Второй уровень представлен повреждениями элементов информационных систем (ИС) и СЗИ $Des_{\{1, 2, 3, \ldots\}}$.

Первый уровень образуют частные сервисы безопасности: сК – конфиденциальность; сЦ – целостность; сД – доступность.

Вершина нулевого уровня K_0 графа G соответствует интегральному критерию ИБ объекта информатизации в целом.

Нечеткая когнитивная модель легко адаптируется к специфическим особенностям организаций путем изменения в графе G множества вершин и связей.

Для описания состояния концептов графа G предлагается использовать лингвистическую переменную «Уровень фактора» и терм-множество ее значений QL.

Вычисление текущих значений факторов в графе G предлагается производить по приведенным ниже формулам (3)–(9):

$$\overline{UZ_j} = UZ_j \cdot \prod_{i=1}^{N} \left(Inv\left(P_i \right) \right)^{\alpha_i}, \tag{3}$$

где $\overline{UZ_j}$ – остаточный (после применения мер защиты P_i) уровень j-й уязвимости; UZ_j – исходный (до применения СЗИ) уровень j-й уязвимости; UZ_j = 1, в случае наличия уязвимости, UZ_j = 0, в случае отсутствия уязвимости; N – количество мер защиты P_i, влияющих на j-ю уязвимость; P_i – интенсивность i-й защитной меры, влияющей на j-ю уязвимость; $\alpha_i \in [0;1]$ – коэффициент снижения уровня j-й угрозы в результате применения i-й защитной меры P_i.

Для нахождения инверсии приращения фактора F предлагается использовать выражение

$$Inv\left(F \right) = \left(1 - \mu\left(F \right) \right), \tag{4}$$

где $\mu(F)$ – функция принадлежности нечеткого числа, соответствующего лингвистическому значению QL_F приращения фактора F.

$$\overline{UG_j} = UG_j \cdot \prod_{i=1}^{L} \left(Inv\left(Z_i \right) \right)^{\beta_i}, \tag{5}$$

где $\overline{UG_j}$ – остаточный (после применения мер защиты Z_i) уровень j-й угрозы; UG_j – исходный (до применения СЗИ) уровень j-й угрозы; UG_j = 1, в случае наличия угрозы, UG_j = 0, в случае отсутствия угрозы; L – количество мер защиты Z_i, влияющих на j-ю угрозу; Z_i – интенсивность i-й защитной меры, влияющей на j-ю угрозу; $\beta_i \in [0;1]$ – коэффициент снижения уровня j-й угрозы в результате применения i-й защитной меры Z_i.

$$A_j = \max_{\left\{ i \mid \delta_j^i \neq 0 \right\}} \left\{ UG_j \cdot UZ_i \right\}, \tag{6}$$

где A_j – уровень j-й атаки; UZ_i– уровень i-й уязвимости,

$$\delta_j^i = \begin{cases} 0 - \text{если для реализации угрозы } UG_j \text{ не требуется наличие уязвимости } UZ_i, \\ 1 - \text{если для реализации угрозы } UG_j \text{ требуется наличие уязвимости } UZ_i. \end{cases}$$

$$Des_j = \max_i \left\{ A_i \cdot pwr_i \right\}, \tag{7}$$

где Des_i – уровень j-го повреждения; $pwr_i \in QL$ – интенсивность влияния i-й атаки на j-е повреждение.

$$K_j = Inv\left(\max_i \left\{ Des_i \cdot \mathrm{int}_i \right\} \right), \tag{8}$$

где K_j – уровень j-го частного сервиса безопасности; Des_i – уровень i-го повреждения, влияющего на j-й сервис безопасности; $\mathrm{int}_i \in QL$ – интенсивность влияния i-го повреждения на j-й сервис безопасности.

$$K_0 = \prod_{i=1}^{3} (K_j)^{1/3}, \quad (9)$$

где K_0 – уровень комплексной безопасности ИС; K_j – уровень *j*-го частного сервиса безопасности.

Состояния мер защиты P_i, входящих в систему комплексного обеспечения ИБ (СКОИБ), определяет ЛПР.

Если P_i не представляет собой совокупность отдельных мер защиты информации (такие P_i назовем «*атомарными*»), то ЛПР задает лингвистическую оценку непосредственно P_i.

Если P_i представляет собой комплекс отдельных мер защиты информации p_j^i (такие меры защиты назовем «*молекулярными*»), то ЛПР задает лингвистическую оценку p_j^i, входящих в P_i. Состояние P_i в этом случае определяется на основе следующих правил:

$$\begin{cases} P_i = \min\{p_j^i\}, \text{ если } \{p_j^i\} \text{ действуют одновременно (параллельно)}, \\ P_i = \prod_{j=1}^{M} (p_j^i)^{\alpha_j}, \text{ если } \{p_j^i\} \text{ действуют последовательно, образуя рубежы защиты}, \end{cases}$$

где P_i – текущее значение, отражающее состояние *i*-й «*молекулярной*» меры защиты; p_j^i – *j*-я мера защиты, входящая в *i*-ю «*молекулярную*» меру защиты; *M* – количество p_j^i образующих P_i; $\alpha_i \in [0;1]$ – коэффициент влияния p_j на P_i.

Поскольку повреждение СЗИ P_i – это нарушение его нормального (соответствующего требованиям ИБ) режима функционирования, то состояние P_i можно определить как инверсию уровня его повреждения, оцененного в методике оценки уровня ИБ.

Для применения НКМ на практике необходимо определить множество весов ребер *S* графа *G*, отражающих степень влияния концептов друг на друга.

Для решения данной задачи в качестве экспертов были привлечены представители правоохранительных и контролирующих органов государственной власти, представители банков и финансово-экономических учреждений, работники организаций, работающих в сфере оказания услуг по обеспечению ИБ, а также преподаватели профильных кафедр АГТУ. Общее количество экспертов составило 9 человек. Итоговые значения были определены коллективно – путем проведения экспертами открытой дискуссии.

Построенная НКМ, так же как и методика оценки уровня безопасности ИА на основе НПП, позволяет оценить уровень ИБ. Полученная при этом оценка будет ниже (не выше) чем оценка, полученная на основе НПП, поскольку при переходе от одного уровня к другому в графе *G* НКМ учитываются максимальные значения уровней угроз, уязвимостей, атак и повреждений.

Данная методика была реализована в виде программного продукта, при помощи которого ЛПР может оценить состояние ИБ и принять обоснованные решения по управлению ее уровнем.

Предложенные методики в совокупности позволяют управлять уровнем ИБ. Методика оценки уровня ИБ на основе НПП дает возможность ЛПР вырабатывать обоснованное суждение о необходимости синтеза управляющих решений для вывода сервисов безопасности на заданный целевой уровень, а нечеткая когнитивная модель дает возможность ЛПР синтезировать данные управляющие решения.

Пример практического применения методик в коммерческой компании, предоставляющей IT-услуги

Проиллюстрируем применение предложенных методик для управления уровнем ИБ в компании ООО «АпГрейд». Основными видами деятельности организации являются: разработка ПО и консультирование в этой области; деятельность по созданию и использованию баз данных и информационных ресурсов; техническое обслуживание и ремонт офисных машин и вычислительной техники.

Оценка текущего уровня информационной безопасности ООО «АпГрейд». *Итерация 0.* Специалистом по ИБ ООО «АпГрейд» (ЛПР) были оценены повреждения на 0-м уровне иерархии: A_1 = НС; B_1 = С; B_2 = ВС; B_3 = В; C_1 = Н; Z_1 = НС; Z_2 = Н; E_1 = Н; E_2 = Н, где, в соответствии с иерархией повреждений, A_1 – повреждения каналов передачи данных; B_1 – повреждения инженерно-технических средств (мер) защиты информации; B_2 – повреждения аппаратных средств (мер) защиты информации; B_3 – повреждения организационно-правовых средств (мер) защиты информации; C_1 – повреждения носителей с резервными копиями данных; Z_1 – повреждения жестких дисков серверов; Z_2 – повреждения элементов обработки данных серверов; E_1 – повреждения жестких дисков рабочих станций; E_2 – повреждения элементов обработки данных рабочих станций.

Далее был осуществлен поиск соответствующих правил в БЗ:

Если ([A_1 = НС]) То ([{1,0} (сД = В)] & [{1,0} (сЦ = ВС)]);

Если ([B_1 = С] & [B_2 = ВС] & [B_3 = В]) То ([{0,9} (сД = С)] & [{0,85} (сЦ = С)] & [{0,9} (сК = Н)]);

Если ([C_1 = Н]) То ({1,0} (сД = В)] & [{1,0} (сЦ = В)]);

Если ([Z_1 = НС] & [Z_2 = Н]) То ([{0,95} (сД = В)] & [{0,85} (сЦ = В)]);

Если ([E_1 = НС] & [E_2 = Н]) То ([{1,0} (сД = В)] & [{1,0} (сЦ = В)]).

Результат оценки состояния сервисов безопасности на 0-м уровне иерархии:

$$\text{сД} = \{\max(0{,}9) = 0{,}9\}\ \left(\min\left(\text{В; С; В; В; В}\right)\right);$$

$$\text{сЦ} = \{\max(0{,}85) = 0{,}85\}\ \left(\min\left(\text{ВС; С; В; В; В}\right)\right);$$

$$\text{сК} = \{\max(0{,}9) = 0{,}9\}\left(\min(\text{Н}) = \text{Н}\right).$$

Поскольку «*узловые*» повреждения находятся не на «*критическом*» уровне (Z_1 = НС < ВС; Z_2 = Н < ВС; E_1 = НС < ВС; E_2 = Н < ВС), то был осуществлен переход на 1-й уровень иерархии.

Итерация 1. Были оценены повреждения на 1-м уровне иерархии: F_1 = Н; G_1 = С.

В БЗ данным значениям соответствуют следующие правила:

Если ([F_1 = Н]) То ([{1,0} (сД = В)] & [{1,0} (сЦ = В)]);

Если ([G_1 = С]) То ([{0,8} (сД = НС)] & [{0,85} (сЦ = С)]).

Результат оценки состояния сервисов безопасности на 1-м уровне иерархии:

$$\text{сД} = \{\max(0{,}8) = 0{,}8\}\left[\min\left(\text{В;НС}\right) = \text{НС}\right];$$

$$\text{сЦ} = \{\max(0{,}85) = 0{,}85\}\left[\min\left(\text{В; С}\right) = \text{С}\right].$$

Поскольку G_1 = С («*узловое*» повреждение имеет «*критический*» уровень), то из дальнейшего рассмотрения исключаются: блок повреждений пользовательского ПО рабочих станций; блок повреждений программных средств СЗИ, установленных на рабочих станциях. Несмотря на это, на следующем уровне иерархии остаются блоки для рассмотрения, поэтому был осуществлен переход на 2-й уровень.

Итерация 2. Оценка повреждений на 2-м уровне иерархии показала, что H_1 = Н; J_1 = Н; J_2 = С; J_3 = В; J_4 = С.

Поиск соответствующих правил в БЗ дал следующий результат:

Если ([H_1 = Н]) То ([{1,0} (сД = В)] & [{1,0} (сЦ = В)]);

Если ([J_1 = Н] & [J_2 = С] & [J_3 = В] & [J_4 = С]) То ([{0,7} (сД = С)] & [{0,8} (сЦ = С) & [{0,9} (сК = НС)]).

Оценка состояния сервисов безопасности на 2-м уровне иерархии:

$$\text{сД} = \{\max(0{,}7) = 0{,}7\}\ \left[\min\left(\text{В; С}\right) = \text{С}\right];$$

$$\text{сЦ} = \{\max(0{,}8) = 0{,}8\}\ \left[\min(\text{В};\ \text{С}) = C\right];$$

$$\text{сК} = \{\max(0{,}9) = 0{,}9\}\left[\min(\text{НС}) = \text{НС}\right].$$

Поскольку «*узловые*» повреждения ниже «*критического*» значения (H_1 = Н < ВС), то был осуществлен переход на 3-й уровень иерархии.

Итерация 3. Оценка повреждений на 3-м уровне иерархии: L_1 = Н.

Соответствующее правило БЗ имеет вид:

$$\text{Если } ([L_1 = \text{Н}])\ \text{То } ([\{1{,}0\}\ (\text{сД} = \text{В})]\ \&\ [\{1{,}0\}\ (\text{сЦ} = \text{В})]).$$

Результат оценки состояния сервисов безопасности на 3-м уровне иерархии:

$$\text{сД} = \{\max(1{,}0) = 1{,}0\}\left[\min(\text{В}) = \text{В}\right];$$

$$\text{сЦ} = \{\max(1{,}0) = 1{,}0\}\ \left[\min(\text{В}) = \text{В}\right].$$

Поскольку текущий (3-й) уровень последний, то был осуществлен переход к вычислению интегральной оценки сервисов безопасности по формуле (2):

$$\text{сК} = \{\max(0{,}9) = 0{,}9\}\left[\min(\text{Н};\ \text{НС};\ \text{НС}) = \text{Н}\right];$$

$$\text{сЦ} = \{\max(0{,}85;\ 0{,}85;\ 0{,}8) = 0{,}85\}\left[\min(\text{С};\ \text{С};\ \text{С};\ \text{В}) = \text{С}\right];$$

$$\text{сД} = \{\max(0{,}8) = 0{,}8\}\ \left[\min(\text{С};\ \text{НС};\ \text{С};\ \text{С}) = \text{НС}\right].$$

Полученные значения отражают текущий уровень ИБ в ООО «АпГрейд».

Результаты оценки оказались неудовлетворительными для ЛПР, поэтому было принято решение о повышении уровня ИБ и осуществлен синтез управляющих решений для вывода сервисов ИБ на необходимый целевой уровень.

Синтез управляющих решений для ООО «АпГрейд». Для решения задачи синтеза управляющих решений специалист по ИБ ООО «АпГрейд» оценил состояние СЗИ, имеющихся в организации:

P_1 – процедура защиты документов при их хранении – min($p_1^{'}$, $p_1^{''}$):

- $p_1^{'}$ – регламент защиты документов при их хранении – НС;
- $p_1^{''}$ – контроль защиты документов при их хранении – НС;

P_2 – процедура контроля за работой пользователей ИС и обслуживающего персонала – min($p_2^{'}$, $p_2^{''}$):

- $p_2^{'}$ – организационные средства контроля за работой пользователей ИС и обслуживающего персонала – С;
- $p_2^{''}$ – технические средства контроля за работой пользователей ИС и обслуживающего персонала – Н;

P_3 – использование сертифицированного лицензионного ПО – В;

P_4 – процедура разграничения доступа к ИА – min($p_4^{'}$, $p_4^{''}$, $p_4^{'''}$):

- $p_4^{'}$ – организационные меры разграничения доступа к ИА – С;
- $p_4^{''}$ – технические меры разграничения доступа к ИА – НС;
- $p_4^{'''}$ – программно-аппаратные меры разграничения доступа к ИА – С;

P_5 – техническая поддержка аппаратных средств – С;

P_6 – поддержка программных средств – С и т. д.

В результате применения программного продукта, реализующего описанную выше методику синтеза управляющих решений для вывода сервисов ИБ на необходимый целевой уровень, на основании информации от ЛПР были получены следующие оценки сервисов ИБ:

– уровень конфиденциальности – Н (индекс схожести Ω = 1);
– уровень целостности – НС (индекс схожести Ω = 0,96);
– уровень доступности – НС (индекс схожести Ω = 0,96).

Было выявлено, что низкий уровень конфиденциальности в первую очередь связан с нарушениями в организации пропускного режима. Эти нарушения могут быть результатом реализации угрозы «Подкуп персонала», которая реализуется через уязвимость «Мотивированность персонала на совершение деструктивных действий». Уровень данной уязвимости может быть снижен путем соответствующей работы с персоналом и путем усиления контроля за работой сотрудников.

На уровень целостности и доступности наибольшее влияние оказали повреждения каналов передачи данных. К этим повреждениям, согласно НКМ, может привести сбой, который, в свою очередь, может произойти из-за низкой надежности каналов. Повысить надежность можно путем усиления работы службы технической поддержки и путем заземления основного и вспомогательного оборудования, используемого при обработке информации.

Полученные данные послужили основанием для разработки рекомендаций по усилению мер, направленных на обеспечение конфиденциальности, целостности и доступности информации. Был усилен контроль над работой сотрудников, проведены тренинги для сотрудников, посвященные ИБ; заземлено основное и вспомогательное оборудование, используемое при обработке информации; усилена специалистами служба технической поддержки и внесены изменения в должностные инструкции работников данной службы.

Реализация указанных превентивных мер защиты, а также ликвидация существующих повреждений ИА и СЗИ позволили повысить уровень конфиденциальности, целостности и доступности до состояния ВС.

Аналогичная работа была проведена в АГТУ (образовательное учреждение), в ООО «Электроспецмонтаж» (коммерческая компания, предоставляющая услуги по электромонтажу), в Астраханском центре «Аэронавигация Юга» (государственная корпорация по организации воздушного движения). Полученные результаты позволили сделать вывод о возможности применения предлагаемой методики в организациях различного профиля.

Заключение

Таким образом, унификация походов позволила разработать методику, которая может быть применена в организациях различного профиля.

Методика позволяет:

– оценить текущий уровень ИБ в организации;
– в случае неудовлетворительных результатов оценки синтезировать управляющие решения для вывода сервисов ИБ на необходимый целевой уровень.

СПИСОК ЛИТЕРАТУРЫ

1. *Ажмухамедов И. М.* Системный анализ и моделирование слабоструктурированных и плохоформализуемых процессов в социотехнических системах / И. М. Ажмухамедов, О. М. Проталинский // Инженерный вестн. Дона // URL: http://www.ivdon.ru/magazine/archive/n3y2012/916.

2. *Авдеева З. К.* Когнитивное моделирование для решения задач управления слабоструктурированными системами (ситуациями) / З. К. Авдеева, С. В. Коврига, Д. И. Макаренко // Когнитивный анализ и управление развитием ситуаций (CASC'2006): Тр. 6-й Междунар. конф. / под ред. З. К. Авдеевой, С. В. Ковриги. М.: Ин-т проблем управления РАН, 2006. С. 41–54.

3. *Максимов В. И.* Когнитивные технологии для поддержки принятия управленческих решений / В. И. Максимов, Е. К. Корноушенко, С. В. Качаев // Технологии информационного общества 98 – Россия»: материалы конф. // URL: http://www.iis.ru/events/19981130/maximov.ru.html.

4. *Борисов В. В.* Нечеткие модели и сети / В. В. Борисов, В. В. Круглов, А. С. Федулов. М.: Горячая линия – Телеком, 2012. 284 с.

5. *Ажмухамедов И. М.* Динамическая нечеткая когнитивная модель оценки уровня безопасности информационных активов вуза / И. М. Ажмухамедов // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2012. № 2. С. 137–142.

Статья поступила в редакцию 5.12.2014,
в окончательном варианте – 12.12.2014

ИНФОРМАЦИЯ ОБ АВТОРАХ

Ажмухамедов Искандар Маратович – Россия, 414056, Астрахань; Астраханский государственный технический университет; канд. техн. наук, доцент; доцент кафедры «Информационная безопасность»; aim_agtu@mail.ru.

Князева Оксана Михайловна – Россия, 414000, Астрахань; ООО «UpGrade»; старший инженер; chobitoksana@mail.ru.

I. M. Azhmukhamedov, O. M. Knyazeva

UNIFICATION OF THE APPROACHES TO CONTROL OF THE LEVEL OF INFORMATION SECURITY IN DIFFERENT ORGANIZATIONS

Abstract. A unified method of the level of information security control is developed; it includes two stages: assessment of the current level of information security based on the fuzzy production rules and synthesis of the control decisions based on the application of fuzzy cognitive modeling to bring information security services to the desired target level. The algorithm for assessment of the level of information security is presented in the form of the iterative process, involving the following steps: verbal assessment of the level of damage; search for the relevant rules in the knowledge base; assessment of the state security services at the current level of the hierarchy according to the rules; identifying and excluding from consideration of the blocks containing the damage, the level of which does not allow identification of some blocks at the next level; calculation of integral evaluation of security services and generalized index of information security of the information object in general. The proposed method of assessment of the level of information security does not provide the solution of generating control solutions for information security services output to the desired target level, since it does not contain information about the cause-and-effect relationships between the observed damage information assets and means of information security threats and vulnerabilities and have made it possible implementation attacks, which in turn led to the observed damage. To solve the problem of the second phase was a model showing the links between the damage information assets and means of information security, threats and vulnerabilities. Assessing the level of information security based on the fuzzy production rules enables the decision maker make an informed judgment about the need for synthesis of control solutions for the withdrawal of security services to the specified target level, and the fuzzy cognitive model allows to synthesize the data management decisions. The technique level management of information security has been tested in several organizations in the various fields of activity. The obtained results led to the conclusion on the applicability of the proposed methodology in organizations in the various fields.

Key words: information security, security services, threat, vulnerability, damage, protection, linguistic variable, fuzzy numbers.

REFERENCES

1. Azhmukhamedov I. M., Protalinskii O. M. Sistemnyi analiz i modelirovanie slabo strukturi-rovannykh i plokho formalizuemykh protsessov v sotsiotekhnicheskikh sistemakh [System analysis and modeling of the poorly structured and badly formalized processes in sociotechnical systems]. *Inzhenernyi vestnik Dona.* Available at: http://www.ivdon.ru/magazine/archive/n3y2012/916.

2. Avdeeva Z. K., Kovriga S. V., Makarenko D. I. Kognitivnoe modelirovanie dlia resheniia zadach upravleniia slabostrukturirovannymi sistemami (situatsiiami) [Cognitive modeling for solution of the issues of control of poorly structured systems (situations)]. *Kognitivnyi analiz i upravlenie razvitiem situatsii (CASC'2006). Trudy 6-i Mezhdunarodnoi konferentsii.* Pod redaktsiei Z. K. Avdeevoi, S. V. Kovrigi. Moscow, Institut problem upravleniia RAN, 2006. P. 41–54.

3. Maksimov V. I. Kornoushenko E. K., Kachaev S. V. Kognitivnye tekhnologii dlia podderzhki priniatiia upravlencheskikh reshenii [Cognitive technologies for managerial decision making support]. *Tekhnologii informatsionnogo obshchestva 98 – Rossiia. Materialy konferentsii.* Available at: http://www.iis.ru/events/19981130/maximov.ru.html.

4. Borisov V. V., Kruglov V. V., Fedulov A. S. *Nechetkie modeli i seti* [Fuzzy models and networks]. Moscow, Goriachaia liniia – Telekom, 2012. 284 p.

5. Azhmukhamedov I. M. Dinamicheskaia nechetkaia kognitivnaia model' otsenki urovnia bezopasnosti informatsionnykh aktivov vuza [Dynamic fuzzy cognitive model of assessment of the level of university information security]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2012, no. 2, pp. 137–142.

The article submitted to the editors 5.12.2014,
in the final version – 12.12.2014

INFORMATION ABOUT THE AUTHORS

Azhmukhamedov Iscandar Maratovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Candidate of Technical Sciences; Assistant Professor; Assistant Professor of the Department "Information Security"; aim_agtu@mail.ru.

Knyazeva Oksana Mikhailovna – Russia, 414000, Astrakhan; Ltd. "UpGrade"; Senior Engineer; chobitoksana@mail.ru.