УДК 330.46; 004.056

ОЦЕНКА УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВЫХ УЧРЕЖДЕНИЙ

Ажмухамедов И.М.[1], Князева О.М.[2], Большакова Л.В.[3]

[1]ФБГОУ ВПО Астраханский государственный технический университет, Астрахань, Россия, (414056, г. Астрахань, ул. Татищева, 16), aim_agtu@mail.ru
[2]ООО «АпГрейд», Астрахань, Россия, (414004, г. Астрахань, ул. Красная набережная, 171),info@upgrade30.ru
[3]ФБГОУ ВПО Астраханский государственный университет, Астрахань, Россия, (414056, г. Астрахань, ул. Татищева, 20А), tanya15101993@yandex.ru

Обеспечение информационной безопасности (ИБ) имеет особое значение для финансовых организаций. Это связано с тем, что нарушение любого из сервисов ИБ приводит к значительным финансовым и репутационным потерям. Решение задачи обеспечения ИБ невозможно без оценки текущего уровня безопасности информационных активов. Существующие методики оценки уровня информационной безопасности не позволяют вырабатывать обоснованные суждения о состоянии конфиденциальности, целостности и доступности информации. В связи с этим целью данной работы явилась разработка методики, которая позволит оценивать состояние сервисов информационной безопасности. В результате исследования предложена методика оценки уровня информационной безопасности на основе применения базы знаний, состоящей из нечетких продукционных правил. Данная методика была применена в финансовой организации, осуществляющей посредническую деятельность в сфере пенсионного страхования. Полученная оценка послужила основанием для разработки рекомендаций по усилению организационно-технических и программно-аппаратных мер защиты информации в финансовой организации.

Ключевые слова: информационные активы, сервисы безопасности, уязвимости, уровень повреждений, лингвистическая переменная, нечеткие числа, база знаний.

LEVEL ASSESSMENT OF INFORMATION SECURITY IN FINANCIAL INSTITUTIONS

Azhmuhamedov I.M.[1], Knyazev O.M.[2], Bolshakov L.V.[3]

[1]Astrakhan State Technical University, Astrakhan, Russia, (414056, Astrakhan, Tatischevast., 16), bert91@mail.ru
[2]Ltd. "Upgrade", Astrakhan, Russia, (414004, Astrakhan, Red embankment st., 171), info@upgrade30.ru
[3]Astrakhan State University, Astrakhan, Russia, (414056, Astrakhan, Tatischevast., 20A), tanya15101993@yandex.ru

Ensuring information security (IS) is of particular importance for financial institutions. This is due to the fact that the breach of any of the services IS leads to significant financial and reputational losses. Solution to the problem of information security is not possible without assessing the current level of security of information assets. Existing methods of assessing the level of information security do not allow to develop informed judgments about the state of the confidentiality, integrity and availability of information. Therefore, the aim of this work was to develop a methodology that will allow to assess the state of information security services. The study proposed a method of estimating the level of information security through the use of a knowledge base consisting of fuzzy production rules. This methodology has been applied in the financial organization engaged in mediation efforts in the field of pension insurance. The resulting estimate was the basis for the development of recommendations for strengthening the organizational, technical and software and hardware protection measures in the financial organization.

Keywords: information assets, security service, vulnerability, the degree of injury, linguistic variable, fuzzynumber, knowledge base.

Информационные активы (ИА), в состав которых входят информационные ресурсы и средства обработки информации, все чаще выступают как источник получения материальных и финансовых благ. При этом в процессе эксплуатации они могут быть подвержены различным угрозам: разрушению, краже, несанкционированному использованию и т.п. В связи с этим задача обеспечения информационной безопасности (ИБ)

становится все более актуальной. Решение данной задачи невозможно без оценки текущего уровня безопасности информационных активов.

Особое значение обеспечение информационной безопасности имеет для финансовых структур (банков, финансовых компаний, брокерских фирм, кредитных кооперативов и т.п.). Нарушение любого из сервисов ИБ приводит в подобных организациях не только к экономическим потерям, но и влечет за собой существенные репутационные риски.

Исследования в области оценки уровня ИБ преимущественно ведутся по двум направлениям: оценка по эталону и оценка на основе вероятности реализации угроз. При этом данные подходы обладают общим недостатком: полученные в результате применения методик значения результирующих показателей не достаточно информативны. Они не позволяют выработать обоснованные суждения о состоянии конфиденциальности, целостности и доступности информации и уровне ИБ в целом.

Постановка задачи

В связи с этим возникает необходимость в разработке методики оценки уровня ИБ, которая позволяет оценивать состояние (уровень) сервисов безопасности.

Решение задачи

Методика должна учитывать, что уровень защищенности информационных активов определяется состоянием основных сервисов безопасности информации: конфиденциальность, целостность, доступность. Состояние сервисов безопасности в свою очередь зависит от интенсивности повреждений ИА и средств защиты информации (СЗИ). Уровень данных повреждений обычно определяется лицом, принимающим решение (ЛПР), на основании наблюдений и формулируется им вербально в виде лингвистических оценок.

Наличие нечеткости при оценке уровня наблюдаемых повреждений, а также при определении интенсивности влияния повреждений на уровень сервисов безопасности, приводит к тому, что задача оценки уровня ИБ становится слабоформализуемой.

Одним из наиболее эффективных подходов при решении слабоформализуемых задач является использование нечеткого когнитивного моделирования (НКМ), неоспоримыми достоинствами которого является возможность формализации численно неизмеримых факторов, использования неполной, нечеткой и даже противоречивой информации [1-3].

Для формализации оценки повреждений информационных активов и средств защиты информации введем лингвистическую переменную «Уровень фактора» и терм-множество ее значений *QL*, состоящее из 5 элементов:

QL = {Низкий (Н), Ниже среднего (НС), Средний (С),
Выше среднего (ВС), Высокий (В)}} (1)

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

$\{\boldsymbol{XX}(a_1, a_2, a_3, a_4)\}$, (2)

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

Применение классификатора позволяет перейти от качественного описания уровня параметра к стандартному количественному виду соответствующей функции принадлежности из множества нечетких трапецеидальных чисел.

Для формализации экспертных суждений, отражающих влияние наблюдаемых повреждений информационных активов и средств защиты информации на уровень сервисов безопасности, используем набор нечетких продукционных правил вида (3), которые образуют базу знаний (БЗ):

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

где:$D_i, S_j \in QL$ – лингвистические оценки уровней 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 (следствия) "$K_j = S_j$" - определяют состояние j-го сервисов безопасности: {K_1 – сервис «Конфиденциальность» *(сК)*;K_2 - сервис «Целостность» *(сЦ)*;K_3 - сервис «Доступность» *(сД)*}; O_jотражает 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.

На этапе формирования БЗ может возникнуть ситуация, когда при высоком уровне одних повреждений невозможно определить уровень других (например, при высоком уровне аппаратных повреждений компьютера невозможно определить уровень повреждений операционной системы, установленной на данном компьютере).

С целью учета данного факта была построена иерархия повреждений, состоящая из 4 уровней и включающая в себя 13 блоков (рисунок 1).

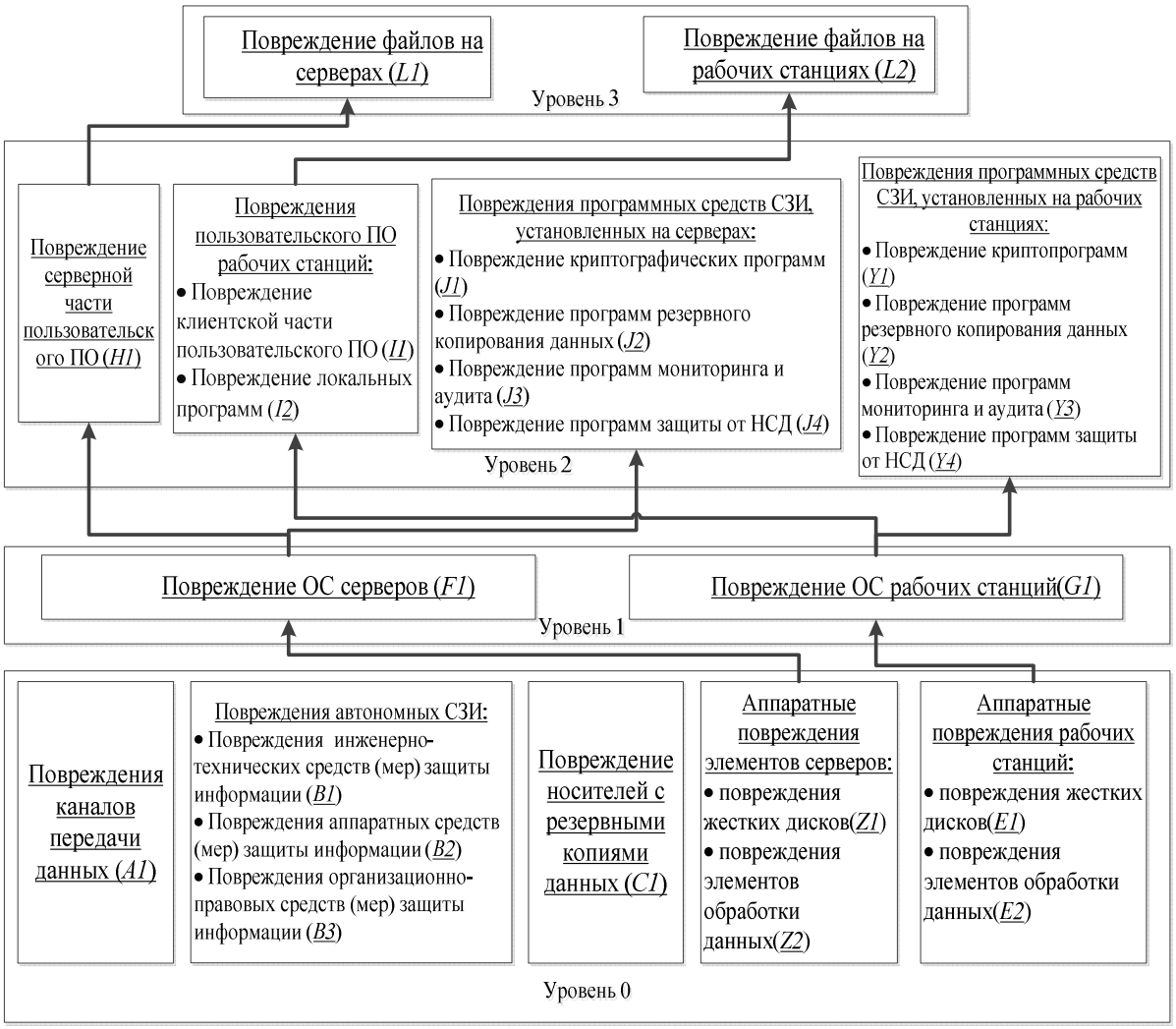

Рис.1. Иерархия повреждений

Нулевой уровень образуют:

1. Блок повреждений каналов передачи данных. Такие повреждения влияют на доступность и целостность информации.

2. Блок физических повреждений элементов серверов. Данные повреждения влияют на доступность и целостность информации.

3. Блок физических повреждений элементов рабочих станций. Эти повреждения влияют на доступность и целостность информации.

4. Блок повреждений автономных (независящих от функционирования элементов информационной системы (ИС)) СЗИ: инженерно-технических и аппаратных средств; правовых и организационных мер защиты информации. Данные повреждения влияют на конфиденциальность, доступность и целостность информации.

5. Блок повреждений носителей с резервными копиями данных. Данные повреждения влияют на доступность и целостность информации.

Первый уровень содержит:

6. Блок повреждений системного программного обеспечения серверов. Данные

повреждения влияют на доступность и целостность информации.

7. Блок повреждений системного программного обеспечения рабочих станций. Данные повреждения влияют на доступность и целостность информации.

На втором уровне расположены:

8. Блок повреждений пользовательского программного обеспечения (ПО) серверов. Данные повреждения влияют на доступность и целостность информации.

9. Блок повреждений пользовательского ПО рабочих станций. Данные повреждения влияют на доступность и целостность информации.

10. Блок повреждений программных средств СЗИ, установленных на серверах. Данные повреждения влияют на конфиденциальность, доступность и целостность информации.

11. Блок повреждений программных средств СЗИ, установленных на рабочих станциях. Данные повреждения влияют на конфиденциальность, доступность и целостность информации.

Третий уровень образуют:

12. Блок повреждений файлов на серверах. Данные повреждения влияют на доступность и целостность информации.

13. Блок повреждений файлов на рабочих станциях. Данные повреждения влияют на доступность и целостность информации.

Построенная таким образом иерархия повреждений отвечает следующим условиям: внутри одного уровня повреждения не влияют друг на друга и повреждения, находящиеся на более низких уровнях иерархии, при определенных условиях могут влиять на возможность идентификации повреждений более высоких уровней.

Каждый из блоков иерархии повреждений при необходимости может быть декомпозирован. При этом должны выполняться перечисленные выше условия.

Для заполнения базы знаний эксперты определяют правила вида:

Если $[Des_i = D_i]$ То $[(O_i)(K_j = S_i)]$, (4)

Данные правила (будем называть их *атомарными*) отражают влияние каждого уровня повреждения элементов в блоках иерархии на сервисы безопасности. Например:

Если (Z_1=Н) То (1.0 (*точно*)) (Сервис «Доступность» (*сД*) =В).

Интенсивность влияния повреждений на сервисы безопасности в атомарных правилах во многом зависит от профиля деятельности организации, поскольку он определяет структуру информационной системы и схемы обработки данных. Так, для финансовых организаций аппаратные повреждения серверов оказывают более сильное влияние на сервисы безопасности, чем аппаратные повреждения рабочих станций.

Полученная таким образом совокупность атомарных правил и образует базу знаний. Общее количество атомарных правил равно 295.

При этом база знаний является: *полной*, поскольку для каждого повреждения (и его уровня) определен логический вывод; *не избыточной*, поскольку ликвидация хотя бы одного правила делает базу знаний неполной; *непротиворечивой*, поскольку исключена ситуация когда два и более правил базы знаний 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. Эксперту необходимо определить «*критические*» уровни «*узловых*» повреждений блоков на каждом уровне иерархии.

Например, для нулевого уровня «*узловыми*» повреждениями являются:

- элементы блока физических повреждений серверов информационной системы, которые при «критическом» (например, выше среднего) уровне не позволяют определить повреждения уровня 1 (состояние повреждений операционных систем серверов), уровня 2 (повреждения пользовательского программного обеспечения серверов, повреждения программных средств защиты информации, установленных на серверах), уровня 3 (повреждения данных на серверах);
- элементы блока физических повреждений рабочих станций информационной системы, которые при «критическом» (например, выше среднего) уровне не позволяют определить повреждения уровня 1 (состояние повреждений операционных систем рабочих станций), уровня 2 (повреждения пользовательского программного обеспечения рабочих станций, повреждения программных средств защиты информации, установленных на рабочих станциях), уровня 3 (повреждения данных на рабочих станциях).

Полученный на основе изложенной методики алгоритм оценки уровня безопасности информационных активов представлен на рисунке 2.

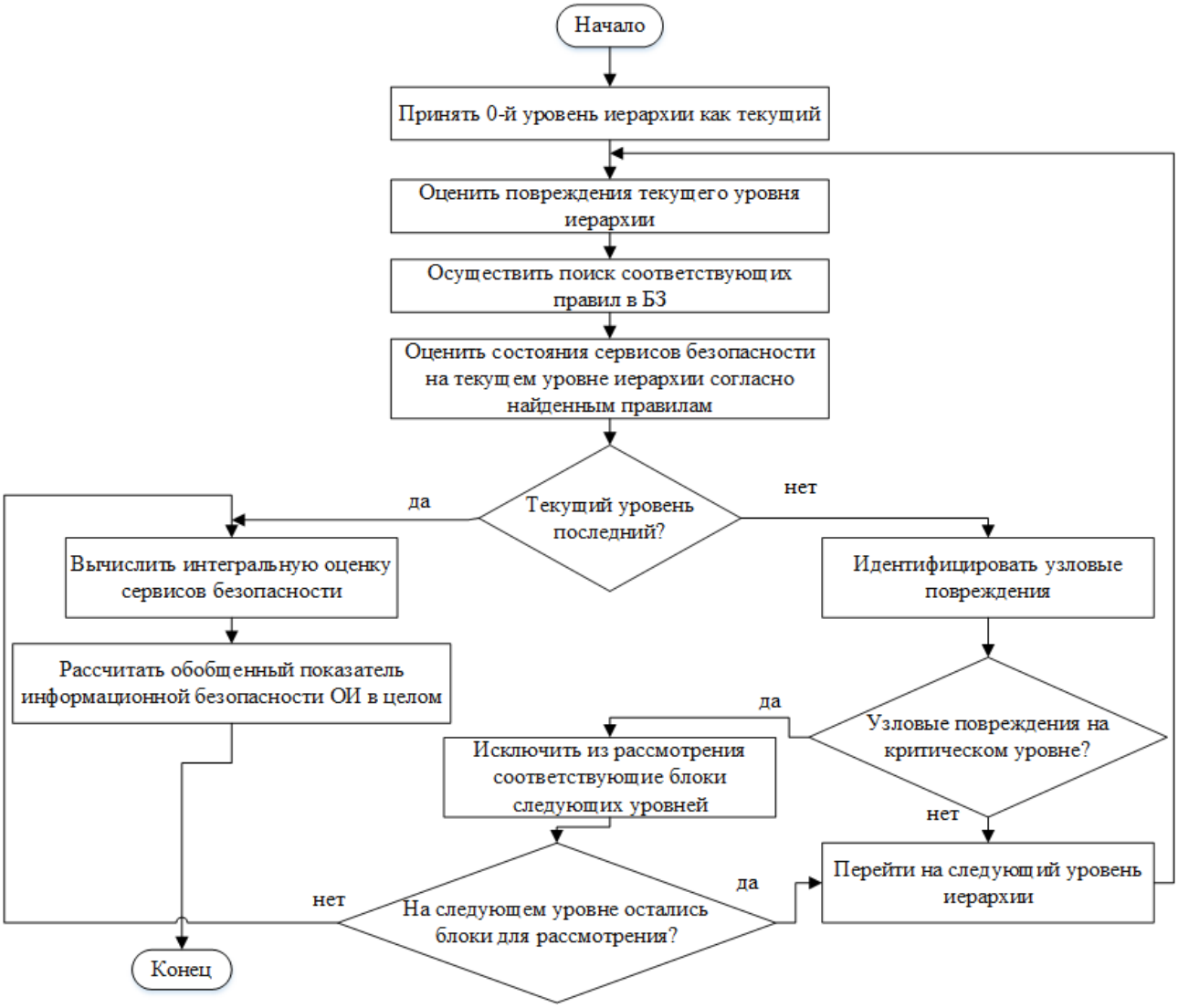

Рис.2. Алгоритм определения уровня безопасности информационных активов

Для оценки состояния сервисов безопасности на каждом уровне иерархии повреждений необходимо воспользоваться процедурой применения правил, образующих базу знаний. Входными данными процедуры являются качественные оценки уровня повреждений ИА и СЗИ на текущем уровне иерархии. На основании данных оценок осуществляется поиск соответствующих атомарных правил в БЗ. Для оценки влияния наблюдаемых ЛПР повреждений *k*-го блока в целом на *j*-й сервис безопасности K_j^k автоматически формируются правила вида (назовем их *блоковыми*):

$$K_j^k: \text{Если } (\&_{i=1}^{W}[Des_i = \bar{D}_i])$$

$$\text{то } (\&_{j=1}^{M}[max_m\{O_m\}_{m\in\{\arg(min_i(\bar{S}_i))\}}(K_j^k = min_i(\bar{S}_i))]), \quad (5)$$

где W – количество повреждений в *k*-м блоке; $\bar{D}_i$– уровень наблюдаемых повреждений Des_i; M – количество сервисов безопасности, на которые влияют повреждения *k*-го блока;$\bar{S}_i$ – определяемое согласно соответствующему атомарному правилу значение сервиса безопасностиK_j при уровне поврежденияDes_i равного $\bar{D}_i$; O_m – степень уверенности эксперта

в оценке влияния повреждения Des_i, имеющего уровень $\overline{D}_i$, на j-й сервис безопасности.

В процессе оценки уровня ИБ автоматически сформируется 5 блоковых правил на нулевом уровне иерархии повреждений; до 2-х правил – на первом уровне; до 4-х правил – навтором уровне; до 2-х правил – на третьем уровне.

Данная процедура определения состояния сервисов безопасности на каждом уровне иерархии с автоматическим формированием блоковых правил позволяет снизить трудоемкость заполнения БЗ экспертом, т.к. ему необходимо сформулировать только атомарные правила. Блоковые правила синтезируются по мере необходимости без участия эксперта. Трудоемкость формирования блоковых правил связана с тем, что при этом эксперту необходимо оценить эффект совокупного влияния нескольких повреждений (их число может достигать 4-х) и их уровней на сервисы безопасности.

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

$$K_j^l : max_m\{O_m\}_{m\in\left\{\arg\left(min_k\left(K_j^k\right)\right)\right\}}[K_j^l = min_k\left(K_j^k\right)], \quad (6)$$

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:

$$K_j : max_m\{O_m\}_{m\in\{\arg(min_k\left(K_j^l\right))\}}[K_j = min_l\left(K_j^l\right)], \quad (7)$$

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

$$K_0 = \prod_{i=1}^{3}(K_j)^{\alpha_i}\,, \quad (8)$$

где K_0 – обобщенный показатель информационной безопасности объекта информатизации в целом; $\alpha_i \in [0;1]$ – коэффициент влиянияK_j на обобщенный показатель информационной безопасности объекта информатизации, $\sum_i^3 \alpha_i = 1$.Применение мультипликативной свертки обусловлено тем, что она в отличие от аддитивной более чувствительна к критериям, имеющим низкие значения.

Для финансовых организаций все сервисы безопасности критично значимы, потеря любого из них может вызвать существенные негативные последствия, поэтому для них примем $\alpha_1 = \alpha_2 = \alpha_3$.

Пример использования методики

Изложенная методика была применена в финансовой организации, осуществляющей

посредническую деятельность в сфере пенсионного страхования.

Для составления базы знаний в качестве экспертов были привлечены специалисты рассматриваемой организации, сотрудники компании «АпГрейд» и преподаватели профильных кафедр Астраханского государственного технического университета (АГТУ) и Астраханского государственного университета (АГУ).

Методом сбора данных было анкетирование. Эксперту предоставлялся список атомарных правил вида (4) с заполненными левыми и пустыми правыми частями:

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

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

…..

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

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

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

Поскольку мнения экспертов оказались хорошо согласованы, итоговые значения уровней сервисов безопасности были найдены путем нахождения моды в совокупности оценок. Степень уверенности эксперта для каждого итогового значения уровня сервиса безопасности была найдена как минимум по всем степеням уверенности, которые были получены для данного итогового значения.

Также эксперты определили «критические» значения «узловых» повреждений блоков на каждом уровне иерархии: для элементов блока физических повреждений серверов ИС критическое значение 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.

Далее был применен алгоритм оценки уровня ИБ, приведенный на рисунке 2.

Итерация 0.

ЛПР оценил повреждения на 0-м уровне иерархии: A_1 = Н; B_1 = НС; B_2 = ВС; B_3 = С; C_1 = В;Z_1 = НС; Z_2 = Н; E_1 = Н; E_2 = Н.

Был осуществлен поиск соответствующих правил в БЗ:

Если (A_1=Н)То(1,0 – *точно*) (*сД*=В);

Если (A_1=Н)То(1,0 – *точно*) (*сЦ=В*);

Если (B_1=НС)То(0,8 – *точно*) (*сК=С*);

Если (B_1=НС)То(1,0 – *точно*) (*сЦ=ВС*);

Если (B_1=НС)То(0,9 – *точно*) (*сД=ВС*);

Если (B_2=ВС)То(1,0 – *точно*) (*сК=С*);

Если (B_2=ВС)То(1,0 – *точно*) (*сЦ=С*);

Если (B_2=ВС)То(0,7 – *весьма возможно*) (*сД=С*);

Если (B_3=С)То(1,0 – *точно*) (*сК=НС*);

Если (B_3=С)То(0,9 – *точно*) (*сЦ=ВС*);

Если (B_3=С)*То (1,0 – точно) (сД=ВС);*

Если *(С1*=С) То (0,9 – *точно) (сД=С);*

Если *(С1*=С) То (0,8 – *точно) (сЦ=ВС);*

Если (Z_1=НС)То(0,9 – *точно*) (*сД=ВС*);

Если (Z_1=НС)То(0,9 – *точно*) (*сЦ=ВС*);

Если (Z_2=Н)То(0,9 – *точно*) (*сД=В*);

Если (Z_2=Н)То(0,9 – *точно*) (*сЦ=В*);

Если (E_1=Н)То(0,9 – *точно*) (*сД=В*);

Если (E_1=Н)То(0,9 – *точно*) (*сЦ=В*);

Если (E_2=Н)То(0,9 – *точно*) (*сД=В*);

Если (E_2=Н)То(0,9 – *точно*) (*сЦ=В*).

В результате выполнения процедуры применения правил, образующих БЗ, были сформированы блоковые правила:

1. Если ([A_1=Н])То([{1,0} (*сД*=В)] &[{1,0} (*сЦ=В*)]);
2. Если([B_1=НС]&[B_2=ВС]&[B_3=С]) То ([{*max*(1,0)=1,0}((*сК=min*(С;С;НС)=НС))] & [{*max*(0,7)=0,7}(*сД=min*(ВС;С;ВС)=С)]&[{max(1,0)=1,0}(*сЦ=min*(ВС;С;ВС)=С)]]);
3. Если ([C_1=С])То([{0,9} (*сД=С*)]& {0,8}(*сЦ=ВС*)]);
4. Если ([Z_1=НС]&[Z_2=Н])То([{0,9}(*сД=min*(ВС;В)=ВС]&[{0,9}(*сЦ= min*(*ВС;В*)]=ВС);
5. Если([E_1=Н]&[E_2=Н]) То [{0,9}(*сД=min*(В;В)=В] &[{0,9}(*сЦ= min*(*В;В*)]);

Конечным результатом применения процедуры являются оценки состояния сервисов безопасности на 0-м уровне иерархии:

сД= {*max*(0,7;0,9) = 0,9} (*min* (В;С;С;ВС;В) = С);

сЦ= {*max*(1,0) = 1,0} (*min* (В;С;ВС;ВС;В) = С);

сК= {*max*(1,0) = 1,0} (*min* (НС) = НС).

Поскольку узловые повреждения находятся не на критическом уровне (Z_1 = НС < ВС; Z_2 = Н < ВС; E_1 = Н < 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 = Н.

Данным повреждениям соответствуют следующие правила в БЗ:

1. Если (F_1=Н)То(1,0 – *точно*) (*сД*=В);
2. Если (F_1=Н)То(1,0 – *точно*) (*сЦ=В*);
3. Если (*G1*=Н) То (0,8 – *точно*) (*сД=В);*
4. Если (G_1=Н)То(1,0 – *точно*) (*сЦ=В*).

В результате выполнения процедуры применения правил, образующих БЗ, были сформированы блоковые правила:

1. Если ([F_1=Н])То([{1,0} (*сД*=В)] &[{1,0} (*сЦ=В*)]);
2. Если ([G_1=Н])То([{0,8} (*сД*=В)] &[{1,0} (*сЦ=В*)]).

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

сД= {*max*(1,0;0,8) = 1,0} (*min* (В;В) = В);

сЦ= {*max*(1,0;1,0) = 1,0} (*min* (В;В) = В).

Поскольку узловые повреждения находятся не на критическом уровне (F_1 = Н<С;G_1 = Н<С), то был осуществлен переход на 2-й уровень иерархии.

Итерация 2

Оценка повреждений на 2-м уровне иерархии показала, что: H_1 = Н;I_1=С;I_2=С; J_1 = Н; J_2 = С; J_3 = В; J_4 = ВС; Y_1 = Н; Y_2 = С; Y_3 = В; Y_4 = ВС.

Был осуществлен поиск соответствующих правил в БЗ:

Если (H_1=Н)То(1,0 – *точно*) (*сД*=В);
Если (H_1=Н)То(1,0 – *точно*) (*сЦ*=В);
Если (I_1=С)То(0,9 – *точно*) (*сЦ*=ВС);
Если (I_1=С)То(0,9 – *точно*) (*сД*=С);
Если (I_2=С)То(0,9 – *точно*) (*сЦ*=НС);
Если (I_2=С)То(0,9 – *точно*) (*сД*=С);
Если (J_1=Н)То(1,0 – *точно*) (*сК*=В);
Если (J_1=Н)То(1,0– *точно*) (*сЦ*=В);
Если (J_1=Н)То(1,0 – *точно*) (*сД*=В);
Если (J_2=С)То(0,8 – *точно*) (*сК*=В);
Если (J_2=С)То(0,8 – *точно*) (*сЦ*=С);
Если (J_2=С)То(0,8 – *точно*) (*сД*=С);
Если (J_3=В)То(0,8 – *точно*) (*сК*=НС);
Если (J_3=В)То(0,8 – *точно*) (*сЦ*=С);
Если (J_3=В)То(0,8 – *точно*) (*сД*=С);

Если (*J4*=ВС) То (0,8 – *точно*) (*сК*=НС);
Если (*J4*=ВС) То (0,8 – *точно*) (*сЦ*=НС);
Если (J_4=ВС)То(0,8 – *точно*) (*сД*=НС);
Если (Y_1=Н)То(1,0 – *точно*) (*сК*=В);
Если (Y_1=Н)То(1,0– *точно*) (*сЦ*=В);
Если (Y_1=Н)То(1,0 – *точно*) (*сД*=В);
Если (Y_2=С)То(0,8 – *точно*) (*сК*=В);
Если (Y_2=С)То(0,8 – *точно*) (*сЦ*=С);
Если (Y_2=С)То(0,8 – *точно*) (*сД*=С);
Если (Y_3=В)То(0,8 – *точно*) (*сК*=НС);
Если (Y_3=В)То(0,8 – *точно*) (*сЦ*=С);
Если (Y_3=В)То(0,8 – *точно*) (*сД*=С);
Если (Y_4=ВС)То(0,8 – *точно*) (*сК*=НС);
Если (Y_4=ВС)То(0,8 – *точно*) (*сЦ*=НС);
Если (Y_4=ВС)То(0,8 – *точно*) (*сД*=НС);

В результате выполнения процедуры применения правил, образующих БЗ, были сформированы блоковые правила:

1. Если ([H_1=Н])То([{1,0} (*сД*=В)] &[{1,0} (*сЦ=В*)]);
2. Если ([I_1=С]&[I_2=С])То([{0,9}(*сД=min*(С;С)=С)]&[{1,0}(*сЦ=min*(ВС;НС)=НС)]);
3. Если ([J_1=Н]&[J_2=С]&[J_3=В]&[J_4=ВС])То([{0,8} (*сК*=НС)] [{0,8} (*сД=НС*)] &[{0,8} (*сЦ=НС*)]);
4. Если ([Y_1=Н]&[Y_2=С]&[Y_3=В]]&[Y_3=ВС])То([{0,8} (*сК*=НС)] [{0,8} (*сД*=НС)] &[{0,8} (*сЦ*=НС)]);

Результат оценки состояния сервисов безопасности на 2-м уровне иерархии:

сК= {*max*(0,8;0,8) = 0,8} (*min* (НС;НС) = НС);

сД= {*max*(0,8;0,8) = 0,8} (*min* (В;С;НС;НС) = НС);

сЦ= {*max*(1,0;0,8;0,8) =1,0} (*min* (В;НС;НС;НС) = НС).

Поскольку узловые повреждения находятся не на критическом уровне (H_1 = Н <ВС; I_1=С<ВС;I_2=С<ВС), то был осуществлен переход на 3-й уровень иерархии.

Итерация 3

Оценка повреждений на 3-м уровне иерархии: L_1 = Н; L_2 = Н;

Соответствующие правила БЗ имеют вид:

Если (L_1=Н)То(1,0 – *точно*) (*сД*=В); Если (*L2*=Н) То (1,0 – *точно*) (*сД*=В);

Если (L_1=Н)То(1,0 – *точно*) (*сЦ*=В); Если (*L2*=Н) То (1,0 – *точно*) (*сЦ*=В).

В результате выполнения процедуры применения правил, образующих БЗ, были сформированы блоковые правила:

1. Если ([L_1=Н])То([{1,0} (*сД*=В)] &[{1,0} (*сЦ=В*)]);
2. Если ([L_2=Н])То([{1,0} (*сД*=В)] &[{1,0} (*сЦ=В*)]).

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

сД= {1,0} (В);

сЦ= {1,0} (В).

Поскольку текущий (3-ий) уровень последний, то был осуществлен переход к вычислению интегральной оценки сервисов безопасности по формуле (7):

сД= {*max*(0,8) = 0,8} [*min* (С;В;НС;В) = НС];

сЦ= {*max*(0,8) = 0,8} [*min* (С;В;НС;В) = НС];

сК= {*max*(1,0) = 1,0} [*min* (Н;Н) = Н].

Для расчета по формуле (8) обобщенного показателя безопасности объекта информатизации в целом был использован программный продукт «Вычисления с нечеткими числами» [4]:

$$K_0 = \prod_{i=1}^{3} (\text{НС} \cdot \text{НС} \cdot \text{Н})^{1/3}$$

Результатом вычислений является нечеткое число с набором узловых точек (0,00;0,00;0,27;0,37), которое можно отнести к категории «Низкий» с индексом схожести 0,62 (индекс схожести категории «Ниже среднего» составляет 0,37).

Полученная оценка послужила основанием для разработки рекомендаций по усилению организационно-технических и программно-аппаратных мер защиты информации в финансовой организации.

Заключение

Разработанная методика оценки уровня ИБ в финансовых учреждениях позволяет: учесть взаимосвязь повреждений ИА и СЗИ в рамках предложенной иерархии; учесть нечеткий характер суждений экспертов о состоянии повреждений и их влиянии на сервисы безопасности.

Оценки, полученные в результате применения разработанной методики, дают возможность лицу, принимающему решения, вырабатывать обоснованное суждение о необходимости синтеза управляющих решений для вывода сервисов безопасности на заданный целевой уровень.

Список литературы

1. Авдеева З.К. Когнитивное моделирование для решения задач управления слабоструктурированными системами (ситуациями) / З. К. Авдеева, С. В. Ковригина, Д. И. Макаренко. М.: Институт проблем управления РАН, 2006. С. 41–54.
2. Ажмухамедов, И.М. Динамическая нечеткая когнитивная модель оценки уровня безопасности информационных активов ВУЗа / И.М. Ажмухамедов // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. 2012. № 2. С.137–142.
3. Ажмухамедов И.М. Информационная безопасность. Системный анализ и нечеткое когнитивное моделирование. М.: Изд-во LAP, 2012. 385с.
4. Ажмухамедов И.М., Колесова Н.А. Вычисления с нечеткими числами // Свидетельство о гос.регистрации программ для ЭВМ №2011614482 Заявка №2011612617 зарегистр. в реестре программ для ЭВМ 7 июня 2011 г.
5. Борисов. В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. М.: Горячая линия-Телеком, 2012. 284 с.

Рецензенты:

Карлина Е.П., д.э.н., профессор, зав. кафедрой «Производственный менеджмент и организация предпринимательства», ФГБОУ ВПО АГТУ, г. Астрахань;

Попов Г.А., д.т.н., профессор, заведующий кафедрой «Информационная безопасность», ФГБОУ ВПО АГТУ, г. Астрахань.