БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 1 (104). – 9–26

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.9 DOI: 10.17212/2782-2230-2022-1-9-26

КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНИВАНИЮ ЗАЩИЩЕННОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА*

В.М. БЕЛОВ[1], Е.Н. ПИВКИН[2], А.А. АРДАЕВА[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, доктор технических наук, профессор кафедры защиты информации. E-mail: vmbelov@mail.ru*
[2] *105066, РФ, г. Москва, ул. Новорязанская, 31/7, к. 2, ПАО АКБ «Связь-Банк», кандидат технических наук. E-mail: evpiv@yandex.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистрант кафедры вычислительной техники. E-mail: nastya.ardaeva@yandex.ru*

Количество событий кибербезопасности в современном мире значительно возросло, из них значительное число приходится на объекты критической информационной инфраструктуры. В настоящей работе рассматриваются основные требования, предъявляемые к моделям оценивания защищенности значимых объектов критической информационной инфраструктуры от несанкционированного доступа, классификация неоднозначной исходной информации, обобщенный алгоритм оценивания уровня защищенности значимых объектов критической информационной инфраструктуры от несанкционированного доступа, нечеткая модель оценивания уровня защищенности с использованием балльной и лингвистической шкал. Определяется порядок проведения оценивания защищенности значимых объектов критической информационной инфраструктуры от несанкционированного доступа. Среди основных требований к моделям оценивания защищенности значимых объектов критической информационной инфраструктуры от несанкционированного доступа выделяют следующие: универсальность, расширяемость, формализуемость, простота, многофакторность. Обобщенный алгоритм оценивания уровня защищенности значимых объектов критической информационной инфраструктуры от несанкционированного доступа включает четыре вычислительных блока: в блоке 1 проводится сбор и первичная обработка информации; в блоке 2 используются вычисления по алгоритмам нечеткого оценивания с лингвистической и балльной шкалами; в блоке 3 оценивается эффективность работы сотрудников по информационной

* Статья получена 02 февраля 2022 г.

безопасности; в блоке 4 осуществляется прогнозирование уровней защищенности значимых объектов критической информационной инфраструктуры от несанкционированного доступа с помощью нечетких временных рядов; в блоке 5 полученные на предыдущих этапах вычислений оценки исследуются с использованием методик обработки результатов данных и делаются соответствующие выводы для принятия решений.

Ключевые слова: модели оценивания защищенности, классификация исходной информации, алгоритм оценивания уровня защищенности, нечеткая модель оценивания уровня защищенности, балльная шкала, лингвистическая шкала, порядок оценивания защищенности, несанкционированный доступ

1. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К МОДЕЛЯМ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ЗО КИИ

Выделяют следующие основные требования к оцениванию уровней защищенности значимых объектов критической информационной инфраструктуры (ЗО КИИ) от несанкционированного доступа [1–14]:

- универсальность – позволяет использовать модель для представления различных типов ЗО КИИ независимо от источника угроз, объекта и средств защиты информации (СЗИ);
- расширяемость – обеспечивает возможность добавления новых характеристик защищенности к модели;
- формализуемость – признак, указывающий на возможность применения математических инструментов для описания параметров модели;
- простота – параметр, который позволяет пользователю легко воспринимать структуру и способы реализации моделируемой защищенности ЗО КИИ;
- многофакторность – позволяет учитывать основные параметры моделируемой защищенности ЗО КИИ.

Исходя из перечисленных требований к оцениванию уровней защищенности ЗО КИИ, были выделены следующие критерии, по которым можно определить эффективность модели оценивания уровней защищенности ЗО КИИ:

- возможность проведения оценивания уровней защищенности ЗО КИИ;
- возможность проведения оценивания уровней защищенности новых ЗО КИИ, описание которых неизвестно;
- возможность идентифицировать процесс вывода результатов применения модели, т. е. возможность более точно определить причины, по которым было принято решение об оценке уровня защищенности ЗО КИИ;
- расширяемость – свойство, позволяющее добавлять в модель дополнительные параметры, которые способны определить различные уровни защищенности ЗО КИИ.

2. КЛАССИФИКАЦИЯ НЕОДНОЗНАЧНОЙ ИСХОДНОЙ ИНФОРМАЦИИ

Проблема выбора альтернатив (принятия решений) – задача, в которой решения принимают в условиях, когда поставленные цели, имеющие ограничения и следствия, порождаются возможными, точно неизвестными действиями. Рассмотрение разнообразных неясных, неопределенных и неточных явлений, событий или фактов, а также связей между объектами и операциями показывает существование различных классов неясности или неопределенности, которые не всегда связаны со случайностью или нечеткостью [1–14].

Имеются признаки необходимости применения нечеткой модели (НМ):

– информация о системе имеет различное качество, а значения параметров оцениваются по разным шкалам;

– нечеткость и неясность выбора или описания границы системы или ее отдельных состояний, а также входных и выходных воздействий;

– для описания функционирования систем в виде эвристических предпочтений используется конструкция естественного языка в виде правил «если – то».

Нечеткая модель при наличии обучающей выборки позволяет аппроксимировать функции или измеряемые данные с любой желаемой точностью [1–14].

Наиболее успешно математическая теория нечеткости представлена нечеткой логикой. Альтернативная теория множеств (АТМ) является уже другой глубокой математической теорией, которая адресована, помимо прочего, также и нечеткости [15–17].

Сложность выбора показателей, позволяющих дать адекватную оценку уровню защищенности ЗО КИИ, определяют:

– необходимостью контроля большого количества средств и объектов защиты, а также мероприятий, направленных на сохранение основных свойств информации (конфиденциальность, целостность, доступность);

– нечеткостью проявления внешних воздействий и внутренних изменений (угрозы, КУИ, нарушители) на ЗО КИИ и системах ее защиты;

– отсутствием аналогов показателей, учитывающих специфику ЗО КИИ и особенности ее функционирования;

– необходимостью получения не только качественной, но и количественной оценки уровня защищенности ЗО КИИ.

Особый интерес представляют такие модели и системы, которые дают возможность эффективно проводить экспертизу (с учетом качественной оценки) и осуществлять выбор наилучшего варианта компьютерной системы, используя интегрированные значения уровней защищенности ЗО КИИ. Такие модели позволяют оценивать уровни защищенности ЗО КИИ и выбирать аль-

тернативы на основе экспертных оценок, эталонных параметров, нечетко определенных исходных данных разработчиков и экспертов, которые представлены как в количественной, так и в лингвистической форме.

3. МЕТОДЫ ОЦЕНИВАНИЯ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ЗО КИИ

Методы оценивания состояния защищенности подразделяют на количественные и качественные (рис. 1) [1–14]. В количественном подходе анализируют степень риска, так как эффективность СЗИ относительно потерь нельзя оценить, если нет количественных показателей степени защищенности.

Качественный подход эффективно применяют в случае, когда потенциальная потеря незаметна, а риск нельзя выразить в денежном эквиваленте. При таком подходе результаты защищенности выражают в лингвистической форме [1–14].

Рис. 1. Методы анализа защищенности ЗО КИИ

Fig. 1. Methods for analyzing the security of the CII

Решая задачи в области ИБ, исследуют корректность работы таких систем в наиболее интересных для специалистов условиях функционирования с заведомо прогнозируемыми значениями параметров, которые адекватно отображают свойства системы.

4. ОБОБЩЕННЫЙ АЛГОРИТМ ОЦЕНИВАНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ

Средства анализа защищенности ЗО КИИ, основанные на нечеткой модели, определяют текущий уровень защищенности ЗО КИИ и позволяют осуществлять прогнозирование динамики его дальнейшего изменения [1–14].

Все перечисленные операции выполняют люди, обладающие совершенными знаниями в области информационной безопасности (ИБ). Но бывают и случаи неполноты знаний, субъективизма предпочтений, неопределенности целей и критериев и т. д. Это особенно заметно при проведении внутреннего аудита (самооценки).

Обобщенный алгоритм оценивания уровня защищенности представляет собой последовательность блоков реализации (рис. 2).

Блок 1 является одним из самых сложных, поскольку требуется произвести сбор, обработку информации, учитывая следующие ограничения:

– нечеткие неполные данные: преобладание качественных данных при небольшом числе количественных, отсутствие предыстории, невоспроизводимость условий угроз, КУИ и атак, ограничения по достижимости точности результата оценки, невозможность сбора исчерпывающих данных;

– нечеткие неполные знания: неадекватность оценки ситуации различными сотрудниками (особенно руководства, отделов информационных технологий, информационной безопасности и других отделов).

Оценивание уровней защищенности ЗО КИИ (блок 2) предполагает использование НМ с лингвистической (НМЛШ) или балльной (НМБШ) шкалами [1–14].

В зависимости от способа представления шкалы, формата шкалы и необходимого быстродействия выбирают одну из НМ.

Различие между полученными оценкой и самооценкой можно рассматривать как элемент для определения эффективности работы сотрудников отдела ИБ (ОИБ). Проведенное обследование является исходной информацией для определения эффективности работы сотрудников по ИБ (блок 3). Причем здесь используют как количественные показатели, так и качественные. В нашей работе блок 3 не анализируется, так как предполагает изучение персональных данных сотрудников ЗО КИИ, на которое требуется специальное разрешение организации.

На основе определенных оценок текущего уровня защищенности и определении эффективности работы сотрудников по ИБ осуществляют прогнозные оценки (блок 4). Прогнозирование осуществляют с использованием модели нечетких временных рядов. В нашей работе блок 4 не используется, так как предполагает наличие персональных данных сотрудников ЗО КИИ из блока 3.

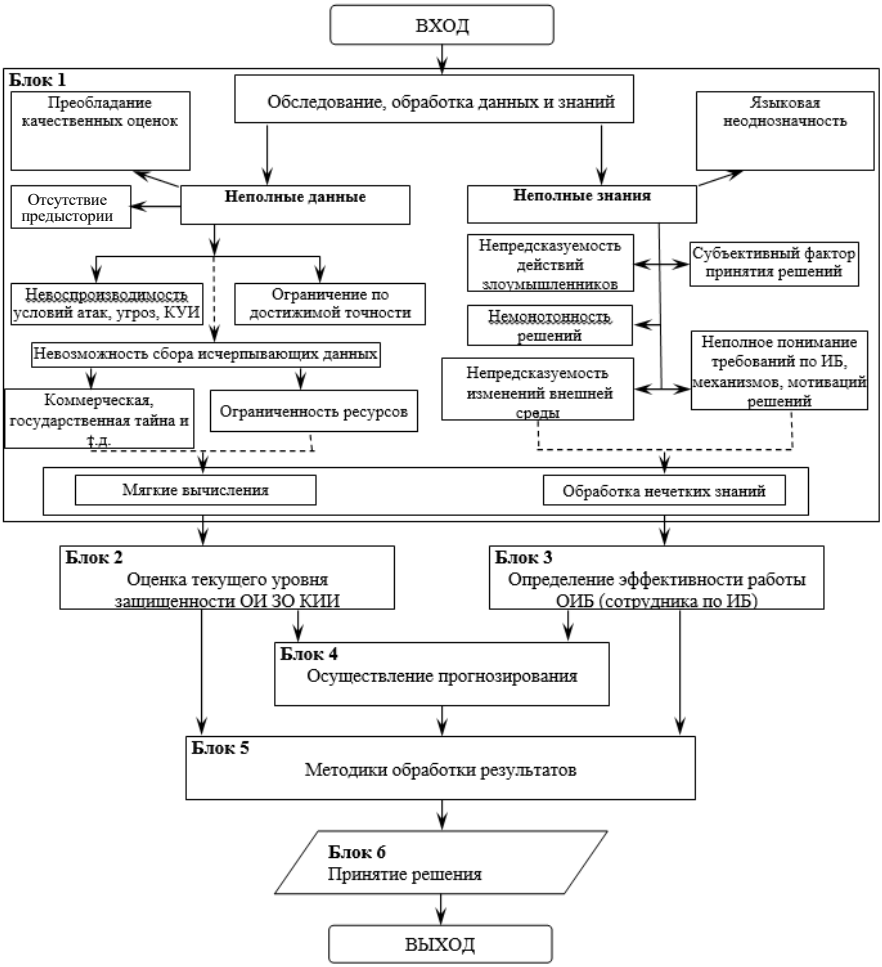

Рис. 2. Обобщенный алгоритм нечеткой модели (комплексный подход)

Fig. 2. Generalized fuzzy model algorithm (complex approach)

Полученные результаты оценок текущего уровня защищенности ЗО КИИ (на основе оценки и самооценки), эффективности работы сотрудников по ИБ, а также прогнозные оценки исследуют с использованием методик обработки

результатов (блок 5) и на их основании делают соответствующие выводы и принимают решения.

5. НЕЧЕТКАЯ МОДЕЛЬ ОЦЕНИВАНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ С ИСПОЛЬЗОВАНИЕМ БАЛЛЬНОЙ ШКАЛЫ

В НМБШ (рис. 3) [1–14] определяет уровень защищенности ЗО КИИ нечеткими термами T_i с использованием лингвистических переменных (ЛП).

Сотрудник по ИБ (ОИБ) отвечает на предварительно ранжированные вопросы. Эти вопросы захватывают всю программу внутреннего аудита ЗО КИИ и ранжируются в соответствии с важностью по *N*-балльной шкале. Через определенный промежуток времени сотрудники просматривают вопросы и варьируют диапазон шкалы $[X_j, \overline{X_j}]$ в зависимости от актуальных угроз модели угроз и нарушителя безопасности информации и каналов утечки информации (КУИ) ЗО КИИ, нормативных документов по ИБ.

Рис. 3. Схема определения уровня защищенности ЗО КИИ, основанная на НМБШ

Fig. 3. Scheme for determining the level of security of the CA of the CII, based on the NMBSH

Диапазон $[X_j, \overline{X_j}]$ $(X_j = 0,\ \overline{X} = N_j)$ изменений параметра X_j^* (где j = [1, n], N_j – максимально возможное количество баллов для каждого вопроса, n – число вопросов) отображается на универсальное множество эталонных нечетких чисел (НЧ) $X_{\text{уз}} = [0, L-1]$ (L – количество эталонов), для которого фиксированное значение $X_j^* \in [\underline{X}_j, \overline{X}_j]$ переводится в соответствующий элемент $X_{\text{уз}\,j}^* \in [0, L-1]$ по формуле

$$X_{\text{уз}\,j}^* = (L-1)\frac{X_j^* - \underline{X}_j}{\overline{X}_j - \underline{X}_j}. \qquad (1)$$

Далее задается функция принадлежности (ФП) $\mu_i^j\left(X_{\text{уз}\,j}^*\right)$ (где $i = [1, L]$) нечеткого терма с i-м номером в треугольном виде [17–30] с учетом коэффициентов важности (КВ) PN_j, $j = [1, n]$, вычисленных по оценкам проверяющих ЗО КИИ для каждого компонента вышеприведенной программы аудиторской проверки внутреннего аудита ЗО КИИ.

На завершающей стадии определяют показатель уровня защищенности ЗО КИИ по следующему логическому выражению:

$$\mu_S\left(X_j^*\right) = \bigvee_{i=1}^{L} \bigwedge_{j=1}^{n} \mu_i^j, \qquad (2)$$

где $i = [1, L]$ – номер терма из базового терм-множества T; $j = [1, n]$ – номер компонента экспертного запроса.

6. НЕЧЕТКАЯ МОДЕЛЬ ОЦЕНИВАНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ С ИСПОЛЬЗОВАНИЕМ ЛИНГВИСТИЧЕСКОЙ ШКАЛЫ

Определение состояния защищенности ЗО КИИ в соответствии с НМЛШ (рис. 4) [1–14] реализуют по результатам опроса сотрудников ОИБ (сотрудника по ИБ), разделы (вопросы) предварительно ранжируют через определение КВ: $P_i (i = [1, n]$, n – количество разделов).

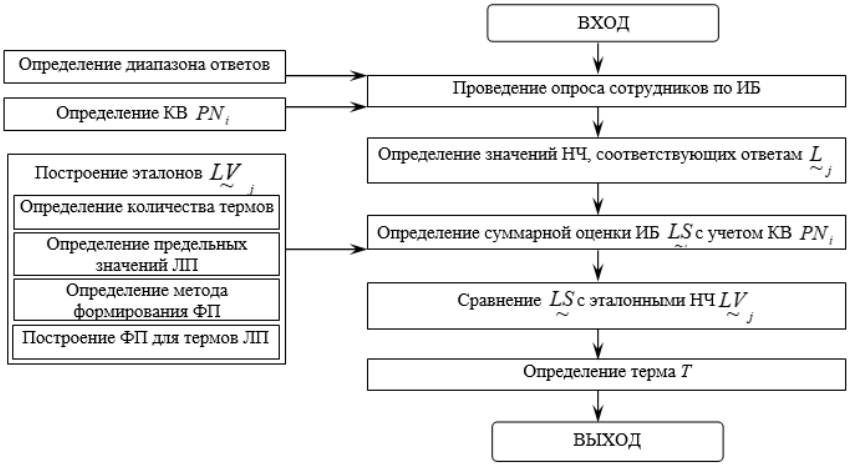

Рис. 4. Схема определения уровня защищенности ЗО КИИ, основанная на НМЛШ

Fig. 4. Scheme for determining the level of security of the CII, based on the NMLSH

Для достижения этой цели используется метод оценивания, основанный на преобразованной матрице $A' = (a'_{vw})$, которая получается из матрицы парных сравнений $A = (a_{ij})$ (см. таблицу). Элементы преобразованной матрицы определяются так:

$$\begin{cases} 100/(a_{ij}+1)a_{ij}, & i<j:\ v=i,\ w=j, \\ a'_{vw}=1, & i<j:\ v=w=i=j, \\ 100/(a_{ij}+1), & i<j:\ v=j,\ w=i, \end{cases} \tag{3}$$

где $i=j=[1,n]$, n – количество разделов (вопросов) программы проверки.

Значения КВ $(P_i, i=[1,n])$ для каждого из вопросов и разделов программы рассчитываются по формуле

$$P_i = \sum_{i=1}^{n} a_{ij} \ \ (i \neq j). \tag{4}$$

Шкала для построения матрицы суждений

Scale for constructing a matrix of judgments

Оценка значимости	Качественная оценка	Примечание
1	Одинаковая значимость	Альтернативы имеют одинаковый ранг
3	Слабое преимущество	Преимущество одной альтернативы перед другой неубедительное
5	Сильное преимущество	Имеются достоверные доказательства значительного преимущества одной альтернативы
7	Очевидное преимущество	Имеются веские доказательства в пользу одной альтернативы
9	Абсолютное преимущество	Имеются веские доказательства в пользу преимущества одной альтернативы перед другой с наибольшей степенью убедительности
2, 4, 6, 8	Промежуточные значения	Используются, если требуется компромисс

После определения КВ осуществляется нормализация по выражению

$$PN_i = P_i \Big/ \left(\sum_{i=1}^{n} P_i \right), \tag{5}$$

для того чтобы выполнялось условие

$$\sum_{i=1}^{n} PN_i = 1 . \tag{6}$$

Помимо ранжирования вопросов и разделов по степени важности сотрудники, осуществляющие проверку, строят нечеткие эталоны, отображающие лингвистическую переменную «Уровень защищенности», которая является образцом для сравнения НЧ.

Модель НМЛШ (рис. 4) предполагает, что группа из N определенного количества сотрудников ОИБ отвечает на n вопросов (n-компонентный

экспертный запрос). По ответам сотрудников ОИБ формируется НЧ $Z_t(t=[1,N])$, которому ставят в соответствие одно из эталонных. Значения НЧ, соответствующие оценке ответов всей группы сотрудников ОИБ на j-й раздел (вопрос) $(j=[1,n])$, определяется по формуле

$$\underset{\sim}{L}_j = \left(\sum_{t=1}^{N} \underset{\sim}{Z}_t \right) \Big/ N, \tag{7}$$

где $\sum$ – нечеткое сложение, выполненное по одному из методов реализации операций нечеткой арифметики [1–14].

Суммарную оценку защищенности определяют с учетом ранее вычисленных КВ:

$$\underset{\sim}{LS} = \left(\sum_{j=1}^{n} PN_i \underset{\sim}{L}_j \right). \tag{8}$$

Образованное $\underset{\sim}{LS}$ сравнивают с эталонными НЧ, для чего используют α-уровневое расстояние (АУР) [16]:

$$d(\underset{\sim}{LS}, \underset{\sim}{LV}_j) = \left(\sum_{\substack{j=1 \; i=1 \\ (\forall X_{\text{уз}y} \geq \alpha)}}^{k \; m} | x_i - y_j | \right) \Big/ k, \tag{9}$$

где α – заданное значение α-уровня $(0 \leq \alpha \leq 1)$; x_i и y_i – носители полученного и эталонного НЧ $\underset{\sim}{LS}$ и $\underset{\sim}{LV}_j$; m – количество компонентов НЧ $\underset{\sim}{LS}$; k – количество компонентов НЧ $\underset{\sim}{LV}_j$ с ФП $\mu_y \geq \alpha$.

Критерием соответствия $\underset{\sim}{LS}$ одному из эталонных НЧ считают минимальное АУР, которое и определяет уровень защищенности ЗО КИИ:

$$d\min_i = \bigwedge_{j=1}^{k} d\left(\underset{\sim}{LS}, \underset{\sim}{LV}_j\right), \tag{10}$$

где $\underset{\sim}{LV}_j$ – эталонные НЧ.

7. ПОРЯДОК ПРОВЕДЕНИЯ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ЗО КИИ

Для проведения оценивания защищенности [1–14] ЗО КИИ предполагается соблюдение следующих этапов.

1. Необходимо провести осмотр ЗО КИИ, анализ документов по ИБ, их актуальность, достоверность, соответствие положений дел в требованиях документов по ИБ России, опрос сотрудников по ИБ и аудит ИБ с целью своевременного выявления, оценивания и прогнозирования источников угроз ИБ, причин и условий, способствующих нанесению ущерба интересам России, нарушению нормального функционирования и развития ИТКС России.

2. Составить вопросы по различным направлениям ИБ. Определить коэффициенты важности, используя метод относительного ранжирования, или руководствоваться требованиями на законодательном уровне.

3. Сформировать эталонные значения уровней защищенности ЗО КИИ методом лингвистических термов.

4. При проведении аудиторской проверки внутреннего аудита организации провести опрос сотрудников по ИБ, в случае необходимости – опрос специалистов других подразделений.

5. Определить суммарную оценку уровня защищенности и провести сравнение со всеми эталонными значениями ЗО КИИ.

ЗАКЛЮЧЕНИЕ

Определение оценки уровня защищенности ЗО КИИ играет важную роль в формировании комплекса практических мер по ее реализации. Но, к сожалению, принятие решения с помощью классических методов и моделей определенно не предполагает желаемого эффекта.

В настоящей работе были рассмотрены основные требования, предъявляемые к моделям оценивания защищенности ЗО КИИ, классификация неоднозначной исходной информации, обобщенный алгоритм оценивания уровня защищенности ЗО КИИ, нечеткая модель оценивания уровня защищенности с использованием балльной и лингвистической шкал, а также определен порядок проведения оценивания защищенности ЗО КИИ.

СПИСОК ЛИТЕРАТУРЫ

1. *Белов В.М., Пивкин Е.Н.* Анализ проблем создания модели комплексной системы защиты информации в региональных налоговых органах // Актуальные проблемы безопасности информационных технологий: материалы I Международной заочной научно-практической конференции / Сибирский государственный аэрокосмический университет. – Красноярск, 2007. – С. 19–21.

2. *Белов В.М., Пивкин Е.Н.* Информационные потоки и способы их формализации с использованием аппарата нечетких множеств в региональных налоговых органах // Инфокоммуникационные системы и технологии: проблемы и перспективы / под ред. А.В. Бабкина. – СПб., 2007. – С. 336–339.

3. *Белов В.М., Пивкин Е.Н., Прокопец В.Д.* Основные математические модели и методы при построении систем защиты информации // Инфокоммуникационные системы и технологии: проблемы и перспективы / под ред. А.В. Бабкина. – СПб., 2007. – С. 300–331.

4. *Белов В.М., Пивкин Е.Н.* Оценка уровня информационной безопасности на основе нечетких моделей с лингвистической шкалой в территориальных налоговых органах // Математическое образование в регионах России: труды Международной научно-практической конференции. – Барнаул: Изд-во АлтГТУ, 2007. – С. 105–108.

5. *Пивкин Е.Н., Белов В.М.* Классификация неоднозначной исходной информации при обеспечении информационной безопасности в территориальных налоговых органах // Управление созданием и развитием систем, сетей и устройств телекоммуникаций: труды научно-практической конференции / под ред. А.В. Бабкина, В.А. Кежаева. – СПб., 2008. – С. 356–362.

6. *Белов В.М., Пивкин Е.Н.* Подход к оценке уровня информационной безопасности в территориальных налоговых органах // Математические методы в технике и технологиях – ММТТ. – 2007. – Т. 10. – С. 239–240.

7. *Капустин А.В., Пивкин Е.Н., Белов В.М.* Оценка уровня информационной безопасности организаций банковской системы на основе аппарата нечетких множеств // Наука и молодежь – 2007: материалы V Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. – Барнаул: Изд-во АлтГТУ, 2008. – С. 13–15.

8. *Шуроватов М.А. Пивкин Е.Н., Белов В.М.* Оценка уровня защищенности виртуального канала на основе аппарата нечетких множеств // Наука и молодежь – 2007: материалы V Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. – Барнаул: Изд-во АлтГТУ, 2008. – С. 5–7.

9. *Пивкин Е.Н., Белов В.М.* Нечеткие модели в системе защиты информации, составляющей налоговую тайну // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2008. – № 2 (18), ч. 1. – С. 125–128.

10. *Белов В.М., Пивкин Е.Н., Прокопец В.Д.* Оценка уровня информационной безопасности на основе нечетких моделей в территориальных налоговых органах // Научно-технические ведомости СПбГПУ. – 2007. – № 4-2 (52). – С. 130–132.

11. *Пивкин Е.Н., Белов В.М.* Современные экспертные нечеткие системы: анализ проблемы применения // Снижение рисков и смягчение последствий чрезвычайных ситуаций природного и техногенного характера – приоритетные направления обеспечения комплексной безопасности населения юга Западной Сибири: материалы Шестой международной научно-практической конференции. – Барнаул: Азбука, 2008. – С. 199–200.

12. *Шуроватов М.А., Пивкин Е.Н., Белов В.М.* Программное обеспечение оценки уровня защищенности виртуального канала // Ползуновский альманах. – 2008. – № 4. – С. 90–93.

13. *Капустин А.В., Пивкин Е.Н., Белов В.М.* Программное обеспечение оценки защищенности объектов информатизации на основе аппарата нечетких множеств и стандарта Банка России // Ползуновский альманах. – 2008. – № 4. – С. 97–100.

14. *Шуроватов М.А. Пивкин Е.Н., Белов В.М.* Анализ методов построения функций принадлежности для оценки уровней информационной безопасности на нечетких множествах // Молодежь. Общество. Современная наука, техника и инновации: тезисы докладов VII Всероссийской научной студенческой конференции с международным участием на иностранных языках (8 мая 2008, г. Красноярск) / Сибирский государственный аэрокосмический университет. – Красноярск, 2008. – С. 61–63.

15. *Vopěnka P.* Mathematics in the alternative set theory. – Leipzig: Teubner, 1979. – 120 p.

16. *Vopěnka P.* Fundamentals to mathematics in the alternative set theory. – Bratislava: Alfa, 1990. – 443 p. – In Slovak.

17. *Novák V.* The alternative mathematical model of linguistic semantics and pragmatics. – New York: Plenum, 1992. – 204 p.

Белов Виктор Матвеевич, доктор технических наук, профессор, профессор кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – применение математических методов в различных областях науки, техники, общества. Имеет более 600 научных публикаций. E-mail: vmbelov@mail.ru.

Пивкин Евгений Николаевич, кандидат технических наук, руководитель направления отдела защиты информации департамента безопасности ПАО АКБ «Связь-Банк». Основное направление научных исследований – применение математических методов в различных областях науки, техники, общества. Автор более 80 публикаций. E-mail: evpiv@yandex.ru.

Ардаева Анастасия Андреевна, магистрант кафедры вычислительной техники Новосибирского государственного технического университета. Область научных интересов – прикладная информатика, информационная безопасность. E-mail: nastya.ardaeva@yandex.ru.

DOI: 10.17212/2782-2230-2022-1-9-26

An integrated approach to assessing the security of significant objects of critical information infrastructure from unauthorized access*

V.M. Belov[1], E.N. Pivkin[2], A.A. Ardaeva[3]

[1] *Novosibirsk State Technical University, Karl Marx Avenue, 20, Novosibirsk, 630073, Russian Federation, doctor of technical sciences, Professor of the department of information security. E-mail: vmbelov@mail.ru*
[2] *PJSC JSCB "Svyaz-Bank", 31/7st. Novoryazanskaya, Moscow, 105066, Russian Federation, candidate of technical sciences, E-mail: evpiv@yandex.ru*
[3] *Novosibirsk State Technical University, Karl Marx Avenue, 20, Novosibirsk, 1630073, Russian Federation, Master's student of the department of computer science. E-mail: nastya.ardaeva@yandex.ru*

The number of cybersecurity events in the modern world has increased significantly, of which a significant number fall on objects of critical information infrastructure. This paper discusses the main requirements for models for assessing the security of significant objects of critical information infrastructure from unauthorized access, classification of ambiguous source information, a generalized algorithm for assessing the level of security of significant objects of critical information infrastructure from unauthorized access, a fuzzy model for assessing the level of security using point and linguistic scales. It also determines the procedure for assessing the security of significant objects of critical information infrastructure from unauthorized access. Among the main requirements for models for assessing the security of significant objects of

* *Received 02 February 2022.*

critical information infrastructure from unauthorized access are the following: versatility, extensibility, formalizability, simplicity, multifactoriality. The generalized algorithm for assessing the level of security of significant objects of critical information infrastructure from unauthorized access includes four computational blocks: in block 1, the collection and primary processing of information is carried out; in block 2, calculations using fuzzy evaluation algorithms with linguistic and point scales are used; in block 3, the effectiveness of information security employees is evaluated; in block 4, the levels of security of significant objects of critical information infrastructure from unauthorized access are predicted using fuzzy time series; in block 5, the estimates obtained at previous stages of calculations are examined using data processing techniques and draw appropriate conclusions for decision-making.

Keywords: security assessment models, classification of initial information, security level assessment algorithm, fuzzy security level assessment model, scoring scale, linguistic scale, security assessment order, unauthorized access

REFERENCES

1. Belov V.M., Pivkin E.N. [Analysis of the problems of creating a model of an integrated information security system in regional tax authorities]. *Aktual'nye problemy bezopasnosti informatsionnykh tekhnologii*: materialy I Mezhdunarodnoi zaochnoi nauchno-prakticheskoi konferentsii [Actual problems of information technology security. Materials of the I International Correspondence Scientific and Practical Conference]. Krasnoyarsk, 2007, pp. 19–21. (In Russian).

2. Belov V.M., Pivkin E.N. Informatsionnye potoki i sposoby ikh formalizatsii s ispol'zovaniem apparata nechetkikh mnozhestv v regional'nykh nalogovykh organakh [Information flows and methods of their formalization using the apparatus of fuzzy sets in regional tax authorities]. *Infokommunikatsionnye sistemy i tekhnologii: problemy i perspektivy* [Infocommunication systems and technologies: problems and prospects]. St. Petersburg, 2007, pp. 336–339.

3. Belov V.M., Pivkin E.N., Prokopets V.D. Osnovnye matematicheskie modeli i metody pri postroenii sistem zashchity informatsii [Basic mathematical models and methods in the construction of information security systems]. *Infokommunikatsionnye sistemy i tekhnologii: problemy i perspektivy* [Infocommunication systems and technologies: problems and prospects]. St. Petersburg, 2007, pp. 300–331.

4. Belov V.M., Pivkin E.N. [Assessment of the level of information security based on fuzzy models with a linguistic scale in the territorial tax authorities]. *Matematicheskoe obrazovanie v regionakh Rossii*: trudy Mezhdunarodnoi nauchno-prakticheskoi konferentsii [Proceedings International scientific-practical conference "Mathematical education in the regions of Russia"]. Barnaul, 2007, pp. 105–108. (In Russian).

5. Pivkin E.N., Belov V.M. [Classification of ambiguous initial information while ensuring information security in the territorial tax authorities]. *Upravlenie sozdaniem i razvitiem sistem, setei i ustroistv telekommunikatsii*: trudy nauchno-

prakticheskoi konferentsii [Management of the creation and development of systems, networks and telecommunications devices. Proceedings of scientific and practical conference]. St. Petersburg, 2008, pp. 356–362. (In Russian).

6. Belov V.M., Pivkin E.N. Podkhod k otsenke urovnya informatsionnoi bezopasnosti v territorial'nykh nalogovykh organakh [Approach to assessing the level of information security in the territorial tax authorities]. *Matematicheskie metody v tekhnike i tekhnologiyakh – MMTT = Mathematical Methods in Technics and Technologies – MMTT*, 2007, vol. 10, pp. 239–240.

7. Kapustin A.V., Pivkin E.N., Belov V.M. [Estimation of the level of information security of organizations of the banking system based on the apparatus of fuzzy sets]. *Nauka i molodezh' – 2007*: materialy V Vserossiiskoi nauchno-tekhnicheskoi konferentsii studentov, aspirantov i molodykh uchenykh [Materials of the V All-Russian scientific and technical conference of students, graduate students and young scientists "Science and youth – 2007"]. Barnaul, 2008, pp. 13–15. (In Russian).

8. Shurovatov M.A. Pivkin E.N., Belov V.M. [Estimation of the security level of a virtual channel based on the apparatus of fuzzy sets]. *Nauka i molodezh' – 2007*: materialy V Vserossiiskoi nauchno-tekhnicheskoi konferentsii studentov, aspirantov i molodykh uchenykh [Materials of the V All-Russian scientific and technical conference of students, graduate students and young scientists "Science and youth – 2007"]. Barnaul, 2008, pp. 5–7. (In Russian).

9. Pivkin E.N., Belov V.M. Nechetkie modeli v sisteme zashchity informatsii, sostavlyayushchei nalogovuyu tainu [Fuzzy models in system of protection of the information containing tax secret]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki = Proceedings of TUSUR University*, 2008, no. 2 (18), pt. 1, pp. 125–128.

10. Belov V.M., Pivkin E.N., Prokopets V.D. Otsenka urovnya informatsionnoi bezopasnosti na osnove nechetkikh modelei v territorial'nykh nalogovykh organakh [Assessment of the level of information security based on fuzzy models in the territorial tax authorities]. *Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta = St. Petersburg State Polytechnical University Journal*, 2007, no. 4-2 (52), pp. 130–132.

11. Pivkin E.N., Belov V.M. [Modern expert fuzzy systems: analysis of the application problem]. *Snizhenie riskov i smyagchenie posledstvii chrezvychainykh situatsii prirodnogo i tekhnogennogo kharaktera – prioritetnye napravleniya obespecheniya kompleksnoi bezopasnosti naseleniya yuga Zapadnoi Sibiri*: materialy Shestoi mezhdunarodnoi nauchno-prakticheskoi konferentsii [Proceedings of the Sixth International scientific-practical conference "Risk reduction and mitigation of the consequences of natural and man-made emergencies – priority areas for

ensuring social security of the population in the South of Western Siberia"]. Barnaul, 2008, pp. 199–200. (In Russian).

12. Shurovatov M.A., Pivkin E.N., Belov V.M. Programmnoe obespechenie otsenki urovnya zashchishchennosti virtual'nogo kanala [Virtual channel security level assessment software]. *Polzunovskii al'manakh = Polzunov Almanac*, 2008, no. 4, pp. 90–93.

13. Kapustin A.V., Pivkin E.N., Belov V.M. Programmnoe obespechenie otsenki zashchishchennosti ob"ektov informatizatsii na osnove apparata nechetkikh mnozhestv i standarta Banka Rossii [Software for assessing the security of informatization objects based on the apparatus of fuzzy sets and the standard of the Bank of Russia]. *Polzunovskii al'manakh = Polzunov Almanac*, 2008, no. 4, pp. 97–100.

14. Shurovatov M.A. Pivkin E.N., Belov V.M. [Analysis of methods for constructing membership functions for assessing information security levels on fuzzy sets]. *Molodezh'. Obshchestvo. Sovremennaya nauka, tekhnika i innovatsii*: tezisy dokladov VII Vserossiiskoi nauchnoi studencheskoi konferentsii s mezhdunarodnym uchastiem na inostrannykh yazykakh [Youth. Society. Modern science, technologies and innovations. Abstracts]. Krasnoyarsk, 2008, pp. 61–63. (In Russian).

15. Vopěnka P. *Mathematics in the alternative set theory*. Leipzig, Teubner, 1979. 120 p.

16. Vopěnka P. *Fundamentals of the mathematics in the alternative set theory*. Bratislava, Alfa, 1990. 443 p. (In Slovak).

17. Novák V. *The alternative mathematical model of linguistic semantics and pragmatics*. New York, Plenum, 1992. 204 p.

Для цитирования:

Белов В.М., Пивкин Е.Н., Ардаева А.А. Комплексный подход к оцениванию защищенности значимых объектов критической информационной инфраструктуры от несанкционированного доступа // Безопасность цифровых технологий. – 2022. – № 1 (104). – С. 9–26. – DOI: 10.17212/2782-2230-2022-1-9-26.

For citation:

Belov V.M., Pivkin E.N., Ardaeva A.A. Kompleksnyi podkhod k otsenivaniyu zashchishchennosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury ot nesanktsionirovannogo dostupa [An integrated approach to assessing the security of significant objects of critical information infrastructure from unauthorized access]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 1 (104), pp. 9–26. DOI: 10.17212/2782-2230-2022-1-9-26.