УДК 330:004.056
DOI 10.52452/18115942_2023_4_18

АНАЛИЗ И ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕС-ПРОЦЕССОВ

П.Б. Болдыревский, Л.А. Кистанова

Болдыревский Павел Борисович, д.ф.-м.н.; проф.; заведующий кафедрой математических и естественно-научных дисциплин
Нижегородского государственного университета им. Н.И. Лобачевского
bpavel2@rambler.ru
Кистанова Людмила Анатольевна, старший преподаватель кафедры экономического анализа и информационных технологий Нижегородского государственного агротехнологического университета
lakistanova@mail.ru

Статья поступила в редакцию 30.08.2023
Статья принята к публикации 26.10.2023

В настоящее время растет количество и частота кибератак на активы организаций и бизнеса. Угрозы становятся всё более изощренными. В защите информационной безопасности ищутся уязвимости, которые помогают злоумышленникам реализовать угрозы и нанести ощутимый ущерб. Поэтому вопрос защищенности информационных активов актуален. Цель данной работы – рассмотрение основных факторов информационной безопасности бизнес-процессов с привлечением инструментария нечёткой логики. Авторами рассмотрены вопросы методологии и методов, применяемых для анализа и оценки рисков информационной безопасности. Выделены основные факторы, влияющие на оценку рисков информационной безопасности, – уязвимость, угроза и ценность актива. Для описания факторов предложен лингвистический подход с применением терм-множеств. Разработана нечёткая экспертная система для анализа и оценки рисков информационной безопасности с использованием пакета прикладных программ MATLAB и пакета расширения Fuzzy Logic Toolbox. Для нечёткого вывода использован алгоритм Мамдани. Полученные результаты оценок рисков информационной безопасности для организаций разного уровня продемонстрировали адекватность предложенной модели. Также данная экспертная система может быть использована для мониторинга и прогнозирования рисков информационной безопасности бизнес-процессов.

Ключевые слова: риски и угрозы информационной безопасности, уязвимость, ценность актива, нечёткая логика, нечёткий логический вывод.

Введение

В связи с возрастающей интеллектуализацией экономической и производственной деятельности общества цена и значимость информационных ресурсов значительно увеличивается [1, 2]. Приобретает значение их сохранность, так как информационные активы субъекта могут подвергаться атакам, использующим уязвимости информационной системы и программного обеспечения компьютеров. Главными уязвимостями открытых систем являются: низкая защищенность внешнего периметра сети, доступного из Интернета; низкая защищенность от проникновения в технологическую сеть; недостатки конфигурации устройств; недостатки сегментации сетей и фильтрации трафика; использование словарных паролей; использование устаревших версий программного обеспечения.

Учитывая, что количество и частота попыток несанкционированного доступа к информации непрерывно возрастает, – так, в первом полугодии 2023 года число кибератак в России увеличилось примерно в два раза [3] и при этом появляются новые виды угроз, – то анализ и оценка величины рисков информационной безопасности являются актуальными и чрезвычайно важными.

Суть анализа состоит в том, чтобы определить имеющиеся риски, оценить их величину и выработать меры по их уменьшению, а также убедиться, что риски заключены в приемлемые рамки [4]. В процессе анализа определяются основные информационные активы и их ценность для организации; идентифицируются имеющиеся угрозы и уязвимости безопасности, а также возможные осуществления угроз; рассчитываются риски, связанные с реализацией угроз безопасности [5]. Самой сложной задачей является определение ценности активов и идентификация угроз и уязвимости безопасности. Очевидно, что полностью защитить ценные информационные активы невозможно, но можно грамотно оценить риски и защитить самое необходимое, сэкономив на остальном.

Оценку рисков информационной безопасности можно выполнить количественными, качественными или смешанными методиками. Для

Рис.1. Алгоритм Мамдани [15]

измерения величины риска и ожидаемого ущерба применяют количественную или качественную оценку. При количественной оценке требуется достаточно большая и достоверная база данных, приближенная к ситуации оцениваемого субъекта, а при качественной оценке присутствует субъективность оценки и повышенная гипотетичность результатов [6]. Но у качественной оценки есть ощутимое преимущество – её можно выполнить с минимальными затратами ресурсов, что позволяет более широко применять этот вид оценки рисков [7].

Нами рассматриваются случаи, когда четко определить величину риска трудно и в этой ситуации лучше всего использовать инструментарий нечёткой логики, имеющий качественную оценку [8]. Следовательно, цель данного исследования состоит в выявлении применимости инструментария нечёткой логики для анализа и оценки рисков информационной безопасности с учетом ценности информационных активов и вероятности их уязвимости и угрозы безопасности. Для моделирования экспертной системы по оценке рисков информационной безопасности нами был использован пакет прикладных программ Fuzzy Logic Toolbox for MATLAB.

Методология и методы

Создателем теории нечётких множеств и нечёткой логики с полным основанием считается профессор Калифорнийского университета (Беркли) Лютфи Аскер Заде. Началом его работ в этой области исследований послужила статья, написанная в 1965 году под названием «Fuzzy sets» («Нечёткие множества»). В этой работе было показано отличие классической теории множеств от теории нечётких множеств, в которых применялась градуированная оценка отношения принадлежности элементов множеству. Это отношение описывалось при помощи функции принадлежности $\mu_A(x)$, где $\mu_A(x)$ указывала степень (уровень) принадлежности элемента x подмножеству A. Если высота нечёткого множества A равна 1 ($\sup \mu_A(x)=1$), то нечёткое множество A – нормально, а при $\sup \mu_A(x)<1$ – субнормально.

Функция принадлежности (Membership Function), имеющая треугольную форму (применяемую нами в экспертной системе), описывается числами (*a, b, c*) и формулой (1), по которой вычисляются значения в точке *x*:

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1-\dfrac{x-b}{c-b}, b\le x\le c\\ 0, x\notin(a;c)\end{cases} \quad (1)$$

Если $(b–a)=(c–b)$, то получается симметричный треугольник и функция принадлежности однозначно задается двумя параметрами из чисел (*a, b, c*).

В теории нечётких множеств важное значение занимают лингвистические переменные, значения которых называются термами, а множество возможных значений – терм-множеством.

Структуру лингвистической переменной можно описать набором (N, T, X, G, M**)**, в котором N – название переменной; T – терм-множество N; X – универсальное множество с базовой переменной x; G – некоторое синтаксическое правило, которое может быть задано в форме бесконтекстной грамматики, порождающей термы множества T; M – семантическое правило, которое позволяет поставить в соответствие каждому новому значению данной лингвистической переменной, получаемому с помощью процедуры G, некоторое осмысленное содержание посредством формирования соответствующего нечеткого множества [9].

В качестве нечёткого логического вывода выбираем алгоритм Мамдани (Mamdani) (рис. 1). Он представляет собой упрощение более общего механизма, который базируется на «нечётком выводе» и обобщенном правиле дедукции (generalised modus ponens).

Алгоритм Мамдани реализован в пакете прикладных программ Fuzzy Logic Toolbox for MATLAB, поэтому это дает возможность использовать его в разработке экспертной системы.

В данном исследовании риск информационной безопасности является функцией угрозы, уязвимости и ущерба, зависящего от ценности актива. Уязвимости неотъемлемы от объекта информатизации и обусловливаются слабостью в системе защиты, что и делает возможной реализацию угрозы [10]. Оценка уязвимости актива по отношению к угрозе определяется степенью простоты или легкости, с какой активу может быть нанесен ущерб [11]. Уязвимость сама по себе не причиняет ущерб, но является условием,

Таблица 1

Описание входных и выходных переменных нечёткой модели

Лингвистические переменные	Название	Вид терм-множества
Входная переменная P(ugr)	вероятность реализации угрозы	VL – очень низкая; L – низкая; M – средняя; H – высокая; VH – очень высокая
Входная переменная P(uyaz)	вероятность наличия уязвимости	VL – очень низкая; L – низкая; M – средняя; H – высокая; VH – очень высокая
Входная переменная A(tsen)	степень ценности актива	VL – очень низкая; L – низкая; M – средняя; H – высокая; VH – очень высокая
Выходная переменная R(ib)	уровень риска информационной безопасности	VL – очень низкий; L – низкий; M – средний; H – высокий; VH – очень высокий

Разработано авторами.

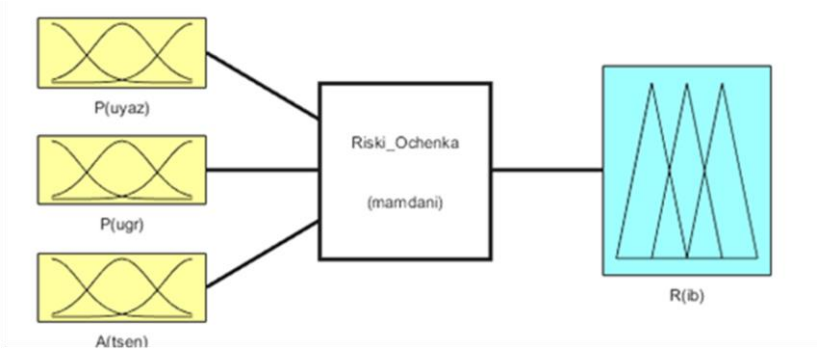

Рис.2. Схема экспертной системы оценки рисков информационной безопасности
Разработано авторами

санкционирующим воздействие угрозы на активы. В противоположность уязвимости угроза обладает способностью наносить ущерб активам и, в критических ситуациях, ущерб организации в целом. Мерой угрозы является вероятность её реализации.

Для того чтобы определить политику информационной безопасности, активы организации необходимо идентифицировать и проранжировать [12]. С точки зрения своей ценности активы должны иметь гарантированную защиту [13]. Таким образом, уровень риска информационной безопасности R(ib) с учетом ожидаемых потерь можно оценить по следующей зависимости:

$$R(ib) = \{P(ugr); P(uyaz); A(tsen)\}, \quad (2)$$

где P(ugr) – вероятность реализации угрозы информационной безопасности; P(uyaz) – вероятность наличия уязвимости; A(tsen) – степень ценности актива.

Определим входные и выходные переменные нечёткой модели, а также их терм-множества, показав полученные данные в таблице 1.

Далее в интерактивном режиме редактора систем нечёткого вывода FIS в пакете прикладных программ Fuzzy Logic Toolbox for MATLAB формируем схему экспертной системы оценки рисков информационной безопасности (рис. 2).

В редакторе функций принадлежности Membership Functions как для входных переменных, так и для выходной переменной задаем форму функций принадлежности, параметры, диапазон [14]. Тип формы функций – треугольный. Диапазон изменения входных переменных – от 0 до 1. Выходная переменная будет оценена нами в диапазоне от 0 до 100. Параметры термов входных переменных будут следующие: VL – очень низкая [0 0 0.25]; L – низкая [0 0.25 0.5]; M – средняя [0.25 0.5 0.75]; H – высокая [0.5 0.75 1]; VH – очень высокая [0.75 1 1]. Параметры термов выходной переменной имеют следующие значения: VL – очень низкий [0 0 25]; L – низкий [0 25 50]; M – средний [25 50 75]; H – высокий [50 75 100]; VH – очень высокий [75 100 100].

На рисунке 3 показано формирование функции принадлежности P(uyaz) вероятности наличия уязвимости как в информационной системе, так и в активе. Параметры выходной переменной – уровень риска информационной безопасности R(ib) для терма H – высокий приведены на рисунке 4.

При составлении системы лингвистических правил вида «если…, то…» используем разработанную для данной экспертной системы методику, характеризующую влияние вероятностей уязвимости, реализации угроз и степени ценности актива на оценку риска информационной безопасности (табл. 2).

Правила IF <условие 1> AND <условие 2> …AND <условие n> THEN <заключение> в разработанной экспертной системе содержат несколько условий. Конъюнктивные правила (conjunction) – правила И или AND требуют одновременного выполнения всех условий [15].

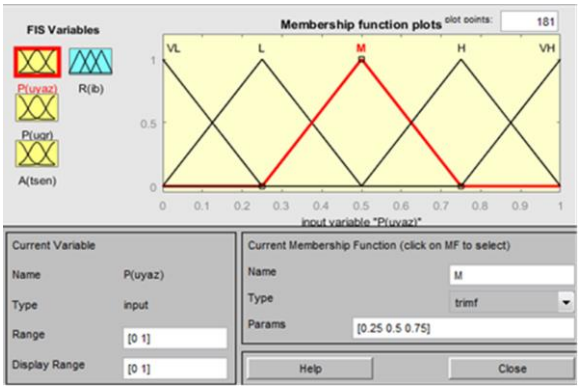

Рис. 3. Данные лингвистической переменной P(uyaz) вероятности наличия уязвимости для терма M – средний
Разработано авторами

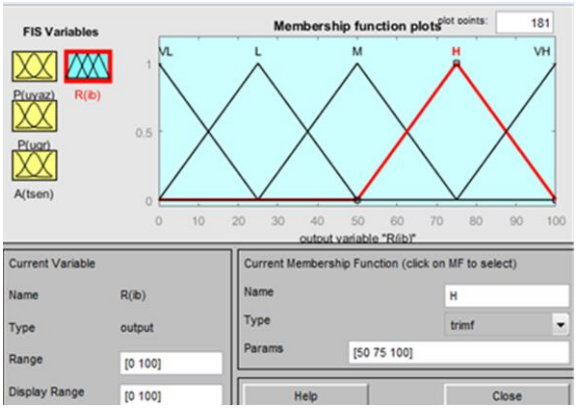

Рис. 4. Параметры выходной переменной уровень риска информационной безопасности R(ib) для терма H – высокий
Разработано авторами

Таблица 2

Правила контроля в экспертной системе

		Вероятность уязвимости и угрозы				
		VH	**H**	**M**	**L**	**VL**
Степень ценности актива	**VH**	VH Риск	VH Риск	H Риск	H Риск	M Риск
	H	VH Риск	H Риск	H Риск	M Риск	M Риск
	M	H Риск	H Риск	M Риск	M Риск	L Риск
	L	H Риск	M Риск	M Риск	L Риск	VL Риск
	VL	M Риск	M Риск	L Риск	VL Риск	VL Риск

VL – очень низкий; L – низкий; M – средний; H – высокий; VH – очень высокий
Разработано авторами

Для этой логической операции используется реализация – нахождение минимума. Заключение содержит оператор, объединяющий объект и значение его характеристики. Весовой коэффициент в логической операции принимается равным 1. С учетом трех входных и одной выходной переменной, а также пяти термов у каждой переменной мы получили 125 правил. Правила в пакете прикладных программ Fuzzy Logic Toolbox for MATLAB были введены при помощи редактора правил нечеткого вывода – Rules, что продемонстрировано на рисунке 5.

Для выполнения процедуры преобразования нечёткого множества в чёткое число – дефаззификации (defuzzification) в реализации нашего алгоритма использовался метод Centroid – центра тяжести. При данном методе обычное значение выходной переменной равно абсциссе точки центра тяжести площади, ограниченной графиком кривой функции принадлежности соответствующей выходной переменной [14].

Значение результирующей переменной рассчитывается по формуле (3):

$$R(ib) = \frac{\int_{Min}^{Max} x * \mu(x)dx}{\int_{Min}^{Max} \mu(x)dx}, \quad (3)$$

где R(ib) – результат дефаззификации; x – переменная, соответствующая выходной лингвистической переменной; $\mu(x)$ – функция принадлежности нечеткого множества, соответствующего

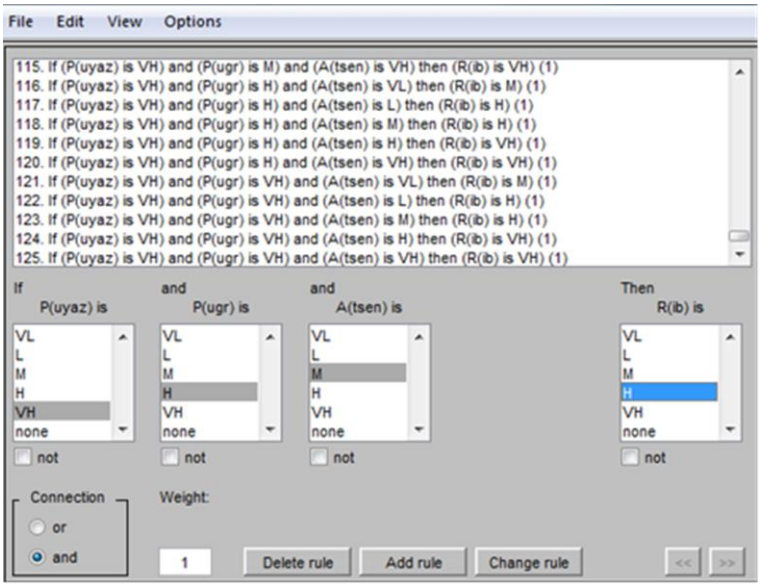

Рис. 5. Сформированная база правил нечеткого вывода в редакторе Rules
Разработано авторами

выходной переменной после этапа аккумуляции; Min и Max – левая и правая точки интервала носителя нечеткого множества рассматриваемой выходной переменной.

Результаты исследования

Особенностью нечёткой экспертной системы является одновременное срабатывание всех заданных правил, с различной степенью их влияния на выходное значение. Поэтому применение данной экспертной системы для прогноза оценки рисков информационной безопасности более чем оправданно, так как соответствует реальным данным в экономике России. Приведем примеры вычислений нечёткого вывода.

Если мы прогнозируем и оцениваем риски информационной безопасности организации малого бизнеса в 2023 году, то характерными составляющими, по оценкам экспертов, будет высокая уязвимость информационных ресурсов P(uyaz)=0.6, вероятность реализации угрозы ниже средней P(ugr)=0.35 (данные организации не так часто подвергаются атакам), средняя степень ценности активов A(tsen)=0.45; уровень тяжести последствий рисков информационной безопасности будет выше среднего и равен R(ib)=60.5%. Это повлечет за собой перебои в работе сервера, в электронной почте, сбои в программном обеспечении, но не затронет репутацию организации (поскольку база контента небольшая).

Для среднего бизнеса количество атак возрастает и вероятность реализации угрозы будет равна P(ugr)=0.5, вероятность уязвимости ресурсов средняя P(uyaz)=0.45, активы, подвергающиеся атакам, имеют среднюю степень ценности A(tsen)=0.5; уровень тяжести последствий рисков информационной безопасности будет средний и равен R(ib)=50%. Это объясняется большей защищенностью информационных активов. Предположительно, данный ущерб не принесёт большие потери, но он может затронуть репутацию организации, что тоже повлечет за собой нежелательные явления.

Положение вещей меняется, когда речь идет о крупной компании, в этом случае даже небольшие повреждения ценных активов, которыми располагает большой бизнес, могут вызвать значительные потери, измеряемые ущербом на десятки миллионов рублей. Если ущерб большой или близок к критическому, то могут нарушиться логистические цепочки, прекратят свое действие договоры, остановится производство, разрушится престиж организации. При этом некоторые ценные активы даже могут быть не восстановлены, например программные продукты и средства связи. Для оценивания рисков информационной безопасности крупной компании выберем следующие параметры: высокую вероятность реализации угрозы – P(ugr)=0.6, вероятность уязвимости ресурсов ниже средней P(uyaz)=0.3; высокую степень ценности активов A(tsen)=0.8, при этом уровень рисков информационной безопасности будет ближе к очень высокому и равен R(ib)=75.7%. Результаты вычислений нечеткого вывода для крупной компании приведены на рисунке 6.

Приведенные примеры использования разработанной нами экспертной системы в среде пакета прикладных программ Fuzzy Logic Toolbox for MATLAB для анализа и оценивания

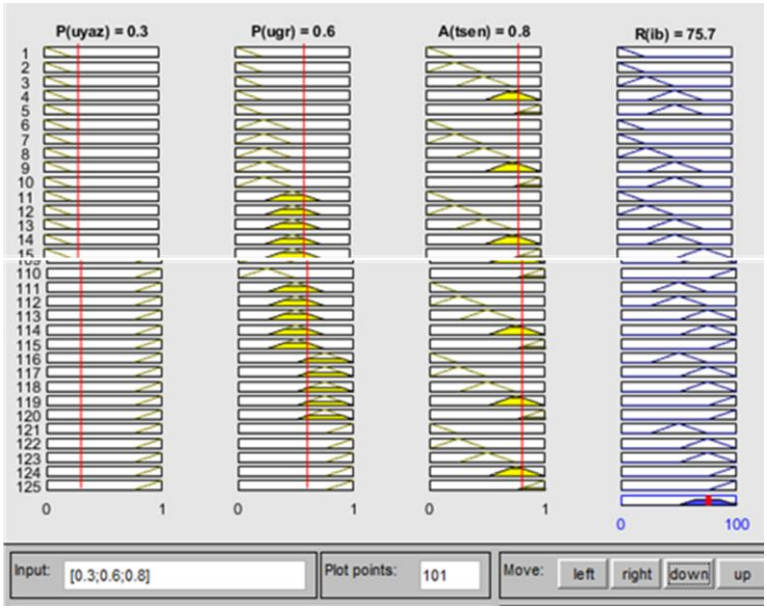

Рис. 6. Результаты вычислений нечёткого вывода для компании крупного бизнеса
Разработано авторами

рисков информационной безопасности демонстрируют применимость её для предсказания ситуации, в которой может оказаться компания или организация, если не будет защищать свои активы и непрерывность бизнеса от вероятностных уязвимостей и кибератак.

Заключение

Доступность программного продукта MATLAB с расширением инструментария нечёткой логики Fuzzy Logic Toolbox и простота его использования по сравнению с другими автоматизированными программами дает возможность применения данной экспертной системы для анализа и оценивания рисков информационной безопасности организации любого масштаба. Недостатки, которые имеются, – зависимость базы данных нечётких правил от входов в систему, статичность и нелинейность нечётких правил, а также невозможность машинного обучения и распознавания образа типа нейронной сети можно нивелировать, если применить автоматизированную экспертную систему в сочетании с системами икусственного интеллекта или нейронными сетями [16].

Таким образом, можно сделать вывод, что при соответствующей настройке полученной экспертной системы при помощи пакета прикладных программ Fuzzy Logic Toolbox for MATLAB для конкретной ситуации в компании нечёткую модель можно использовать не только для анализа и оценки рисков информационной безопасности, но и в мониторинге и в прогнозировании рисков [17].

Список литературы

1. Веллман Р., Заде Л.А. Принятие решений в расплывчатых условиях // Вопросы анализа и процедуры принятия решений. М.: Мир, 1976.

2. Болдыревский П.Б. Основные элементы системы управления рисками промышленных предприятий // Вестник Нижегородского университета им. Н.И. Лобачевского. 2013. № 3 (3). С. 31–34.

3. Число кибератак в России и в мире // Positive Technologies [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/ (дата обращения: 05.07.2023).

4. Садриева А.С. Методы нечеткой логики в оценке рисков информационной безопасности // Материалы IX Международной студенческой научной конференции «Студенческий научный форум». URL: https://scienceforum.ru/2017/article/2017039603 (дата обращения: 30.06.2023).

5. Пашков Н.Н., Дрозд В.Г. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии // Современные научные исследования и инновации. 2020. № 1 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2020/01/90380 (дата обращения: 31.07.2023).

6. Тимошина Н.В., Комарова О.В. Современные проблемы количественной оценки рисков // Киберленинка [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/sovremennye-problemy-kolichestvennoy-otsenki-riskov/viewer (дата обращения: 01.08.2023).

7. Чекудаев К.В. Качественные методы оценки риска. URL: https://rtmtech.ru/articles/metodika-otsenki-riska/?ysclid=lljomew3kt784553514 (дата обращения: 31.07.2023).

8. Болдыревский П.Б., Игошев А.К., Кистанова Л.А. Оценка рисков инновационных процессов // Экономический анализ: теория и практика. 2018. Т. 17. № 8 (479). С. 1465–1475.

9. Корнев Л.В. Нечеткая модель оценки рисков информационной безопасности и поддержки уровня

защищенности ERP-систем // Молодой ученый. 2021. № 27 (369). С. 48–54.

10. Муханова А.А., Ревнивых А.В., Федотов А.М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестник Новосиб. гос. ун-та. Серия: Информационные технологии. 2013. Т. 11. Вып. 2. С. 55–72.

11. Баранова Е.К., Гусев А.М. Методика анализа рисков информационной безопасности с использованием нечеткой логики на базе инструментария MATLAB // Образовательные ресурсы и технологии. 2016. № 1 (13). С. 88–96.

12. Киселева И.А., Искаджян С.О. Информационные риски: методы оценки и анализа // ИТпортал. 2017. № 2 (14). URL: http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/ (дата обращения: 28.06.2023).

13. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».

14. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб.: БХВ-Петербург, 2005. 736 с.

15. Штовба С.Д. Проектирование нечетких систем средствами MATLAB. М.: Горячая линия – Телеком, 2007. 288 с.

16. Кузнецов Ю.А., Перова В.И., Эйвазова Э.Н. Нейросетевое моделирование динамики инновационного развития регионов Российской Федерации // Региональная экономика: теория и практика. 2014. Т. 12. № 4. С. 18–28.

17. Рахматуллина Э.И. Анализ и оценка рисков производственного процесса с применением методов искусственного интеллекта // Молодой ученый. 2021. № 36 (378). С. 11–14. URL: https://moluch.ru/archive/378/83928/ (дата обращения: 28.06.2023).

ANALYSIS AND ASSESSMENT OF INFORMATION SECURITY RISKS

***P.B. Boldyrevskii*[1], *L.A. Kistanova*[2]**

[1]Lobachevsky State University of Nizhny Novgorod
[2]Nizhny Novgorod State Agrotechnological University

Currently, the number and frequency of cyber attacks on the assets of organizations and businesses is growing. Threats are becoming more sophisticated. In the protection of information security, vulnerabilities are being sought that help attackers implement threats and cause tangible damage. Therefore, the issue of security of information assets is relevant. In this article, attention is paid to information security and the problem of analysis and assessment of information security risks with the use of fuzzy logic tools is considered. The issues of methodology and methods used for the analysis and assessment of information security risks are considered. A qualitative assessment method has been chosen. The main factors influencing the assessment of information security risks are highlighted – vulnerability, threat and asset value. A linguistic approach using term sets is proposed to describe the factors. A fuzzy expert system has been developed for the analysis and assessment of information security risks using the MATLAB application software package and the Fuzzy Logic Toolbox extension package. The Mamdani algorithm is used for fuzzy inference. The obtained results of information security risk assessments for organizations of different levels demonstrated the adequacy of the proposed model. Also, this expert system can be used to monitor and predict information security risks.

Keywords: information security risks, information security threats, vulnerability, asset value, fuzzy logic, fuzzy logical conclusion.