УДК 004.056.57

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ ПРОЕКТИРОВАНИИ МЕХАНИЗМА ИНТЕГРИРОВАННОЙ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

[1]Надеждин Е.Н., [2]Щипцова Е.И., [3]Шершакова Т.Л.

[1]Государственный научно-исследовательский институт информационных технологий и телекоммуникаций, Москва, e-mail: e.nadezhdin@informika.ru;

[2]Шуйский филиал Ивановского государственного университета, Шуя, e-mail: elena_shipcova@mail.ru;

[3]Филиал НОУ ВПО «Московский институт государственного управления и права», Смоленск, e-mail: tshershakova@mail.ru

Статья посвящена проблеме анализа корреляции событий безопасности в корпоративной информационной системе. Проанализированы сущность, особенности проявления и количественной оценки корреляционных связей уязвимостей программного обеспечения на этапе проектирования подсистемы интегрированной защиты сетевых ресурсов. Для определения взаимосвязи уязвимостей программного обеспечения на практике используют методы математической статистики и метод экспертных оценок. Указанные методы критичны к объёму и достоверности исходных данных. В статье предложен нечёткий когнитивный подход к определению корреляции уязвимостей, обладающий универсальностью и высокой устойчивостью к вариации исходных данных. Разработана формальная модель механизма обеспечения защиты программного обеспечения на основе использования нечётких когнитивных карт. Для иллюстрации предложенного подхода представлен пример экстрагирования концептов и цепочек концептов, которые характеризуют состояние защищённости компонентов программного обеспечения.

Ключевые слова: информационная система, программное обеспечение, уязвимость, корреляция уязвимостей, нечёткая когнитивная карта

ANALYSIS OF SOFTWARE VULNERABILITY IN THE DESIGN OF THE INTEGRATED MECHANISM OF PROTECTION OF ENTERPRISE INFORMATION SYSTEM

[1]Nadezhdin E.N., [2]Schiptsova E.I., [3]Shershakova T.L.

[1]State Institute of Information Technologies and Telecommunications, Moscow, e-mail: e.nadezhdin@informika.ru;

[2]Shuya branch of Ivanovo state University, Shuya, e-mail: elena_shipcova@mail.ru;

[3]Moscow Institute of State management and law, Smolensk branch, Smolensk, e-mail: tshershakova@mail.ru

The article is devoted to the problem of analyzing the correlation of security events in a corporate information system. The essence, peculiarities of manifestation and quantitative estimation of correlations of software vulnerabilities at the design stage of the subsystem of integrated protection of network resources are analyzed. To determine the relationship between software vulnerabilities in practice use the methods of mathematical statistics and the method of expert assessments. These methods are critical to the scope and validity of source data. The article offers a fuzzy cognitive approach to the determination of the correlation of vulnerabilities, which has the versatility and high resistance to the variation of the initial data. Developed a formal model of the protection mechanism of software based on the use of fuzzy cognitive maps. To illustrate the proposed approach, an example is presented of extracting concepts and chains of concepts that characterize the state of protection of software components.

Keywords: information system, software, vulnerability, correlation of vulnerability, fuzzy cognitive map

Высокие темпы информатизации социально-экономических процессов неизбежно сопровождаются ростом напряжённости в области информационной безопасности (ИБ). Сегодня злоумышленники перешли на новый технологический уровень подготовки и реализации кибернетических атак. Их инструменты максимально удобны и эффективны, а прибыль, получаемая в результате «освоения» активов жертвы, постоянно растет. Внедрение новейших сетевых технологий в сферу управления бизнесом увеличило число потенциальных уязвимостей, которыми могут воспользоваться злоумышленники. При этом действия киберпреступников становятся все более организованными, целенаправленными и изощрёнными, создавая реальную угрозу для бизнеса [1–3]. Последствиями таких атак могут быть: нарушения доступности сетевых сервисов, остановка бизнес-процессов, потеря репутации, понижение лояльности vip-клиентов, недополучение (или полная потеря) прибыли компании. Реалии современного информационного общества настоятельно требуют создания в каждой орга-

низации интегрированной системы защиты информации (СЗИ) [4–6].

На сегодняшний день наиболее востребованы СЗИ, позволяющие увеличить степень интеллектуальности уже существующих механизмов защиты: межсетевых экранов, сканеров безопасности, систем обнаружения вторжений, средств контроля доступа к операционным системам и приложениям. В области управления событиями ИБ получила развитие новая категория защитных систем, реализующих ***концепцию безопасного управления событиями*** (*Security Event Management* – SEM) [2, 3]. Эти системы автоматически соединяют и согласуют между собой регистрационные данные по корпоративной безопасности, получаемые от различных защитных устройств, оценивают их корреляцию, позволяя аналитикам информационной безопасности сосредоточиться на нетривиальных критических задачах.

Применительно к защите информации можно сказать, что *корреляция – это процесс интерпретации, комбинации, сравнения и анализа данных, которые поступают от различных механизмов защиты информации, производимый с целью определения попыток несанкционированного доступа к защищаемым информационным ресурсам либо нападения на них.* В своей основе корреляция событий базируется на следующей теоретической предпосылке: *одно событие, происходящее в течение определенного временного промежутка, является причиной другого события.* В технологическом процессе корреляции событий безопасности выделим следующие задачи:

а) транспортировку данных;

б) нормализацию данных;

в) сжатие (сокращение) данных;

г) построение цепочки прохождения событий;

д) обнаружение шаблонов в событиях;

ж) установление взаимосвязи событий ИБ.

В общем случае все системы корреляции событий осуществляют преобразование потока событий ИБ в полезную информацию, которая содержит данные о состоянии информационной инфраструктуры и выявленных в её среде уязвимостях. Эта информация предъявляется администратору безопасности для принятия решения.

В существующих механизмах корреляции событий безопасности нашли применение следующие подходы [1, 3, 5]: корреляция на основе правил (*rule-based reasoning – RBR*), корреляция на основе моделирования (*model-based reasoning – MBR),* корреляция на основе метода кодовых книг (*codebook*), корреляция с использованием интеллектуальных методов (*artificial intelligence*). Каждый из этих методов обладает рядом недостатков, лимитирующих его применение в режиме реального или регламентного времени.

По мнению экспертов ИБ, этап корреляции является сегодня самой критической частью сложного процесса анализа угроз [2]. Это обусловлено тем, что в рамках классического подхода, базирующегося на инсталляции большого количества не связанных друг с другом средств защиты, уже невозможно обеспечивать аналитиков службы ИБ полной информацией об атаке, которую они должны изучить и ранжировать по степени важности. В то же время как технология корреляция представляет собой развитие целостного подхода к управлению угрозами в гетерогенной среде и требует расхода значительных ресурсов КИС.

Основу постановки и решения задач определения корреляции событий ИБ составляют теория и методы моделирования, математической статистики и экспертных оценок [3, 6, 7].

В открытых научных публикациях используемые алгоритмы и процедуры корреляции, как правило, не конкретизируются. С большой долей вероятности можно предположить, что строго формализованных универсальных методов анализа, систематизации и установления корреляции событий ИБ пока не существует. Обобщая доступные материалы в области управления событиями ИБ, отметим, что основные трудности здесь обусловлены высоким уровнем неопределённости возможных угроз, большим количеством уязвимостей программного обеспечения (ПО) и сложностью мониторинга функциональности объектов автоматизации. В этих условиях закономерным шагом в решении проблемы корреляции является попытка применить апробированный метод нечёткого когнитивного моделирования и анализа, основанный на использовании нечётких когнитивных карт (НКК) [8].

Целью статьи является обоснование нечёткого когнитивного подхода к оцениванию корреляции событий ИБ, обусловленных реализацией информационных атак через уязвимости программного обеспечения корпоративной информационной системы (КИС), на основе применения технологии нечётких когнитивных карт В.Б. Силова.

Уязвимости программного обеспечения будем понимать как критические ошибки, не выявленные в ходе тестирования и не декларированные спецификацией разработчика или заложенные преднамеренно, предоставляющие злоумышленникам исключительные возможности по разглашению информации, её модификации, блокированию использова-

ния и безостаточному уничтожению без возможности восстановления [7, с. 20].

НКК обеспечивают корректность формального отображения слабо структурированной предметной области и приемлемую для практики точность моделирования процессов по сравнению с классическими, знаковыми когнитивными картами. Понятие нечеткой когнитивной карты В.Б. Силова представляет собой расширение классического понятия когнитивной карты, основанное на предположении, что взаимовлияния между концептами могут различаться по интенсивности, и их интенсивность может изменяться с течением времени [8]. Для этого в НКК вводят показатель интенсивности влияния и от классического отношения переходят к нечеткому отношению W, элементы $w_{i,j}$ которого характеризуют направление и степень интенсивности (вес) влияния между концептами e_i и e_j:

$$w_{i,j} = w(e_i, e_j),$$

где w – нормированный показатель интенсивности влияния (характеристическая функция отношения W), обладающий рядом специальных свойств.

НКК отображает исследуемый объект в виде взвешенного ориентированного графа, вершины которого соответствуют элементам множества E (концептам), а дуги – ненулевым элементам отношения W, т.е. причинно-следственным связям. Каждая дуга имеет вес, задаваемый соответствующим значением $w_{i,j}$. Отношение W представимо в виде когнитивной матрицы $W = \{w_{i,j}, i, j = \overline{1,n}\}$ размерности $(n \times n)$ (n – число концептов в системе), которая будет интерпретироваться как матрица смежности данного графа. *Состояние системы* в текущий момент времени определяется набором значений всех концептов НКК. Целевое состояние системы задается вектором значений множества целевых концептов.

Процесс когнитивного анализа событий ИБ при этом включает несколько этапов.

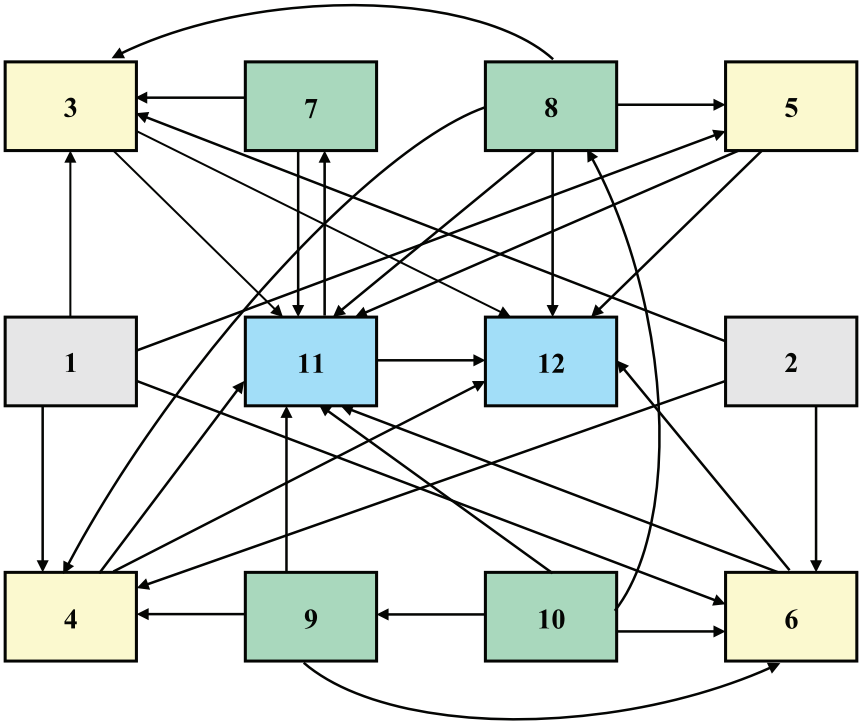
В результате опроса группы экспертов выделяют n существенных факторов (далее – *концептов*), влияющих на защищённость ПО. Эти концепты разделим на четыре группы (табл. 1). Для определённости задачи исследования воспользуемся списком наиболее распространённых дефектов (уязвимостей и неточностей) ПО [7, с. 22].

На следующем этапе на основе экспертных оценок определяют причинно-следственные связи между концептами с выделением их направленности. Результатом таких действий является построение когнитивной карты модели формирования риска информационной безопасности (МФР ИБ) в виде ориентированного графа (рис. 1), формально отражающего причинно-следственные связи без учёта интенсивности взаимовлияний концептов.

Таблица 1

Сводная матрица концептов когнитивной модели

№ п/п	Наименование концепта	Наименование концепта
А. Угрозы		
1	Внешние атаки	e_1
2	Внутренние (инсайдерские) атаки	e_2
Б. Дефекты программного обеспечения		
3	Переполнение буфера [9, с. 50]	e_3
4	Ошибки при работе с динамической памятью [7, с. 21]	e_4
5	Программные закладки	e_5
6	Утечки данных; нарушение целостности информационных ресурсов [7, с. 21]	e_6
В. Технологии защиты от реализации уязвимостей программного обеспечения		
7	Защита на уровне компилятора [7, с. 26]	e_7
8	Специальные инструменты для защиты системных и прикладных ресурсов [7, с. 26]	e_8
9	Система обфускации (запутывания) [7, с. 27]	e_9
10	Контроль целостности исполняемых программ на основе анализа их активности и их обновление [9, с. 52]	e_{10}
Г. Ожидаемые эффекты		
11	Качество функционирования программного обеспечения	e_{11}
12	Риски информационной безопасности, обусловленные нарушением работоспособности программного обеспечения	e_{12}



Когнитивная карта модели формирования риска ИБ

Для количественной оценки силы влияния концептов друг на друга привлекаются эвристические методы, использующие статистику киберпреступлений и обобщающий опыт борьбы с ними. Итогом таких исследований является когнитивная матрица $W = \{w_{i,j}, i, j = \overline{1, n}\}$ (табл. 2), дополняющая НКК (рисунок). Элементы когнитивной матрицы определяются как усреднённые (по числу экспертов) оценки интенсивностей влияния концептов друг на друга. В полученной НКК представлены наиболее существенные, непосредственные связи между концептами. Для реализации методики когнитивного анализа причинно-следственной структуры и характеристик МФР ИБ необходима информация о неявных проявлениях влияния концептов друг на друга и на результат работы ПО.

В интересах количественной оценки опосредованного взаимовлияния концептов требуется выполнить операцию транзитивного замыкания когнитивной матрицы.

Из множества известных способов транзитивного замыкания матрицы смежности воспользуемся алгоритмом, рекомендуемым в работе [8, с. 99]. Известный алгоритм заключается в следующем.

1. От исходной когнитивной матрицы (см. табл. 2) переходят к когнитивной матрице положительных связей R размерностью $(2 \cdot n \times 2 \cdot n)$ на основе процедуры замены:

$$\text{если } w_{i,j} > 0, \text{ то } r_{2i-1,\,2j-1} = w_{i,j},\ r_{2i,\,2j} = w_{i,j};$$
$$\text{если } -w_{i,j} > 0, \text{ то } r_{2i-1,\,2j} = -w_{i,j},$$
$$r_{2i,\,2j-1} = -w_{i,j}.$$

Остальные элементы матрицы R принимают нулевое значение.

2. *Определяют транзитивное замыкание нечёткого отношения* R в соответствии с выражением [8, с. 29]:

$$\tilde{R} = \bigcup_{i=1}^{n} R^i = R \cup R^2 \cup \ldots \cup R^n, \text{ где } R^2 = R \times R.$$

Произведение нечётких отношений вычисляют согласно процедуре:

$$\text{если } D = A \times B,$$
$$\text{то } d_{i,j} = \max_{k=1,\ldots n} a_{i,k} \cdot b_{k,j},\ i, j = 1, \ldots n.$$

3. От вспомогательной матрицы $\tilde{R}$ переходят к транзитивно замкнутой когнитивной матрице V, элементами которой будут пары $(v_{i,j}, \tilde{v}_{i,j})$, где $v_{i,j}$ и $\tilde{v}_{i,j}$ характеризуют соответственно силу положительного и отрицательного влияния i-го концепта на j-й концепт:

$$v_{i,j} = \max\,(r_{2i-1,2j-1}, r_{2i,2j});$$

$$\tilde{v}_{i,j} = -\max\,(r_{2i-1,2j}, r_{2i,2j-1}).$$

Таблица 2

Когнитивная матрица $W = \{w_{i,j}, i, j = \overline{1, 12}\}$ модели формирования риска ИБ

Номер концепта	1	2	3	4	5	6	7	8	9	10	11	12
1	0	0	0,85	0,25	0,81	0,35	0	0	0	0	0	0
2	0	0	0,92	0,87	0	0,96	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	–0,83	0,95
4	0	0	0	0	0	0	0	0	0	0	–0,50	0,81
5	0	0	0	0	0	0	0	0	0	0	–0,65	0,96
6	0	0	0	0	0	0	0	0	0	0	–0,18	0,88
7	0	0	–0,45	0	0	0	0	0	0	0	0,64	0
8	0	0	–0,92	–0,48	–0,35	0	0	0	0	0	0,47	–0,91
9	0	0	0	–0,41	0	–0,63	0	0	0	0	–0,05	0
10	0	0	0	0	0	–0,69	0	0,30	0,15	0	0,18	0
11	0	0	0	0	0	0	0,15	0	0	0	0	–0,75
12	0	0	0	0	0	0	0	0	0	0	0	0

Таблица 3

Результаты расчёта системных показателей нечёткой когнитивной карты

№ п/п	Показатели консонанса		Показатели диссонанса		Показатели влияния		Показатель централизации влияния
	$\vec{H}_i$	$\vec{H}_j$	$\vec{D}_i$	$\vec{D}_j$	$\vec{P}_i$	$\vec{P}_j$	W_i
1	0,583	0	0,417	1	0,188	0	0,188
2	0,500	0	0,500	1	0,229	0	0,229
3	0,333	0,884	0,667	0,116	0,004	0,016	–0,011
4	0,333	0,417	0,667	0,583	0,022	0,007	0,015
5	0,333	0,250	0,667	0,750	0,021	0,030	–0,008
6	0,333	0,333	0,667	0,667	0,057	–0,0008	0,058
7	0,333	0,879	0,667	0,121	–0,016	–0,001	–0,015
8	0,500	0,083	0,500	0,917	–0,148	0,025	–0,173
9	0,391	0,083	0,609	0,917	–0,114	0,013	–0,127
10	0,738	0	0,262	1	–0,092	0	–0,092
11	0,333	0,879	0,667	0,121	–0,048	–0,141	0,094
12	0	0,905	1	0,095	0	0,165	–0,165

4. Вычисляют два базовых показателя НКК:

а) воздействие *i*-го концепта на *j*-й концепт

$$h_{i,j} = \operatorname{sgn}(v_{i,j} + \tilde{v}_{i,j}) \cdot \max(|v_{i,j}|, |\tilde{v}_{i,j}|), \ |v_{i,j}| \neq |\tilde{v}_{i,j}|; \quad (1)$$

б) консонанс влияния *i*-го концепта на *j*-й концепт

$$c_{i,j} = \frac{|v_{i,j} + \tilde{v}_{i,j}|}{|v_{i,j}| + |\tilde{v}_{i,j}|}, \quad (2)$$

который выражает меру доверия к знаку воздействия.

С использованием полученных данных вычисляют системные показатели консонанса и воздействия. Формулы для их определения представлены в работе [8, с. 102].

5. *Анализ результатов расчётов и обоснование рекомендаций.*

В соответствии с приведёнными выше расчётными соотношениями на основании полученной транзитивно замкнутой когнитивной матрицы $V = [(\nu_{i,j}, \tilde{\nu}_{i,j}), \ i, j = \overline{1, n}]$ вычисляют частные (1) и (2), а также системные показатели нечёткой когнитивной модели.

Учитывая, что методология формального представления и анализа проблемной ситуации с применением НКК представлена в монографии В.Б. Силова [8], а некоторые примеры её приложений описаны в авторских статьях [10, 11], акцентируем внимание на вопросах идентификации МФР ИБ. Примем условие, что в результате изучения предметной области экспертами ранее был выделен набор базовых факторов (концептов), оказывающих существенное влияние на защищённость программного ресурса КИС (табл. 1).

В табл. 3 представлены значения системных показателей нечёткой когнитивной модели МФР ИБ (далее – *системы*).

Анализ результатов когнитивного анализа свидетельствует о доминирующем положительном влиянии **концептов** e_4, e_5 и e_6 и отрицательном влиянии **концептов** e_8 и e_9 на составляющую риска ИБ, обусловленную уязвимостями программного и, частично, информационного обеспечения КИС. Представим краткие комментарии к результатам вычислительного эксперимента (см. табл. 3). **Концепты 1** и **2**, характеризующие внешний и внутренний источники информационных атак, в рамках предложенной модели не испытывают целенаправленного воздействия со стороны СЗИ. Поэтому показатели влияния системы соответственно равны нулю: $\bar{P}_1 = 0$ и $\bar{P}_2 = 0$. Аналогично можно указать на **концепт 10**, который в нашем случае представляет собой автономное средство мониторинга и контроля качества функционирования программного обеспечения. По данным когнитивного анализа на величину риска ИБ оказывает относительно сильное влияние **концепт 6** – «Утечки данных» ($\bar{P}_6$ = 0,057), а влияние же системы на концепт практически отсутствует ($\bar{P}_6$ = – 0,0008). Отметим также, что нарушение целостности информационных ресурсов может быть следствием хорошо подготовленных внешних и внутренних атак (**концепты 1** и **2**), осуществляемых согласованно или независимо.

Значительным потенциалом ($\vec{P}_8$ = – 0,148) для нейтрализации выделенных уязвимостей (**концепты 3, 4 и 5**) обладает **концепт 8** «Специальные инструменты защиты системных и прикладных ресурсов». В контексте предложенной модели к таким ресурсам относятся общее и прикладное ПО. Практическая реализация функционала концепта 8 потребует отбора части вычислительных ресурсов. Поскольку данное обстоятельство уменьшит информационную производительность КИС и замедлит скорость выполнения прикладных процессов, влияние концепта 8 на систему будем интерпретировать как снижение качества функционирования программ. При этом относительно высокий консонанс концепта 8 ($\vec{H}_8$ = 0,5) подчёркивает стабильность указанной закономерности.

Ослабленное влияние **концепта 3** «Переполнение буфера» ($\bar{P}_3$ = 0,004) на систему – модель формирования риска ИБ – можно объяснить компенсацией данной уязвимости совокупностью механизмов защиты, представленных **концептами 7 и 8**.

Выводы

1. Опираясь на результаты проведённого когнитивного анализа, можно предположить, что наибольший положительный эффект следует ожидать от согласованного изменения группы управляемых концептов НКК, которые находятся в цепочке причинно-следственной связи и в совокупности обеспечивают устойчивое воздействие на систему – МФР ИБ.

2. Модель формирования риска ИБ, обусловленного осуществлением информационных атак через характерные уязвимости ПО КИС, позволяет решить ряд прикладных задач, которые характерны для корреляции событий ИБ. Несмотря на укрупнённый характер модели и упрощённое когнитивное отображение связей между концептами, в рамках предложенного подхода можно идентифицировать существенные связи между уязвимостями и видовыми механизмами защиты ПО.

3. Формальное представление модели МФР ИБ в виде НКК позволило систематизировать знания предметной области, статистические данные об инцидентах ИБ и опыт экспертов в интересах выявления закономерностей и количественной оценки степени корреляции разнородных уязвимостей и мер защиты на риски ИБ.

4. Полученные результаты исследования могут стать методической основой для выбора направления модернизации существующей системы управления событиями безопасности с целью полного удовлетворения требований политики корпоративной безопасности в условиях изменяющихся характеристик внешних и внутренних угроз.

Список литературы

1. Мухин В.Е., Волокита А.Н. Анализ событий информационной безопасности для проведения корректирующих действий по управлению безопасностью // Информатика, управление и вычислительная техника. – 2009. – № 50. – С. 1–7.

2. Гарусев М. Системы корреляции событий: революция или эволюция? // Сетевой журнал. – 2003. – № 7 [Электронный ресурс]. – URL: http://www.setevoi.ru/cgi-bin/text.pl/magazines/2003/7/30 (дата обращения: 08.09.2017).

3. Федорченко А.В. Анализ методов корреляции событий безопасности в SIEN-системах. Часть 2 / А.В. Федорчен-

ко, Д.С. Левшун, А.А. Чечулин, И.В. Котенко // Труды СПИИ РАН. – 2016. – № 6(49). – С. 208–225.

4. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 Магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. Специальный выпуск. – 2015. – № 5(13). – С. 2–10.

5. Козлова Е.А. Оценка рисков информационной безопасности с помощью метода нечёткой кластеризации и вычисления взаимной информации // Молодой учёный. – 2013. – № 5. – С. 154–161.

6. Надеждин Е.Н., Новикова Т.Л. Оптимизация поиска уязвимостей в системе защиты ресурсов информационно-вычислительной сети университета // Современные наукоёмкие технологии. – 2017. – № 4. – С. 38–43.

7. Аветисян А. И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. – 2014. – № 3(4). – С. 20–28.

8. Силов В.Б. Принятие стратегических решений в нечеткой обстановке: монография. – М.: ИНПРО-РЕС, 1995. – 228 с.

9. Уланов А.В. Уязвимости программного обеспечения – одна из основных угроз информационной безопасности современных информационно-телекоммуникационных систем // Бизнес и безопасность в России. – 2010. – № 56. – С. 49–53.

10. Надеждин Е.Н. Нечёткая когнитивная модель механизма обеспечения конкурентоспособности программного продукта // Austrian Journal of Technical and Natural Sciences. Scientific journal. – 2016. – № 1–2. – P. 13–19.

11. Надеждин Е.Н., Смирнова Е.Е. Когнитивный анализ механизма формирования экономической компетентности выпускника университета// Современные проблемы науки и образования. – 2016. – № 2; URL: http://www.science-education.ru/article/view?id=24174 (дата обращения: 10.08.2017).