УДК 004.056.53
DOI: 10.12737/23243

Е.Э. Аверченкова, Д.И. Гончаров, Д.А. Лысов

МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СОВЕТУЮЩЕЙ СИСТЕМЫ

Рассмотрены вопросы обеспечения информационной безопасности разрабатываемой автоматизированной системы. Сформулирована модель угроз безопасности. Определены актуальность и возможность реализации угроз, уровень проектной защищенности разработанной информационной системы. Рассмотрены особенности формирования модуля информационной безопасности и его взаимосвязь с другими элементами структурно-функциональной схемы автоматизированой системы.

Ключевые слова: информационная безопасность, информационная советующая система, модель.

E.E. Averchenkova, D.I. Goncharov, D.A. Lysov

MODEL OF INFORMATION SECURITY OF INFORMATION ADVISING SYSTEM

The problems in assurance of information security for the automated system under development are considered. The model of threats to security is formulated. A topicality and possibility of threats realization, a level of design protection of the information system developed are defined. Peculiarities in the formation of an information security module and its correlation with other elements of a structural-functional circuit of an automated system are considered.

Key words: information security, information advising system, model.

Введение

Автоматизация управленческой деятельности широко применяется в современном бизнесе. Область ее применения связана с производством, маркетингом, финансами и позволяет на основе анализа ретроспективных данных принимать управленческие решения. Однако использование автоматизирующих управленческую деятельность программных продуктов требует обеспечения информационной безопасности. Определение угроз безопасности информации должно носить систематический характер и осуществляться как на этапе создания информационной системы и формирования требований по ее защите, так и в ходе эксплуатации информационной системы. Систематический подход к определению угроз необходим для определения потребности в конкретных требованиях к защите информации и создании адекватной эффективной системы защиты информации в информационной системе. Меры защиты автоматизированной системы должны обеспечивать эффективное и своевременное выявление и блокирование угроз безопасности информации, в результате реализации которых возможно наступление неприемлемых негативных последствий.

Предметная область исследования

Система информации, формируемой внешней средой и поступающей к региональной социально-экономической системе, характеризуется повышенной сложностью, неоднородностью и противоречивостью [7]. Таким образом, при принятии управленческих решений на региональном уровне менеджерам следует опираться на собственные профессиональные навыки, прошлый опыт, интуицию.

Однако при сложных и нечетко сформулированных задачах опора только на интуицию увеличивает риск принятия неверного или неоптимального решения. Актуальность исследования вопросов проектирования советующих систем связана с

тем, что в настоящее время отсутствуют единые методики и технологии их создания. Кроме того, необходимо отметить несовершенные методы проектирования баз знаний советующих систем, основанных на нечетком характере хранимой экспертной информации [5]. Следовательно, автоматизация поддержки принятия решений выступает направлением оптимизации управленческой деятельности.

Теоретическим и практическим вопросам проектирования интеллектуальных систем посвящены работы зарубежных ученых - Левина Р., Дрангга Д., Таусенда К., Нейлора К., Форсайта Р. и др., а также отечественных авторов - Гавриловой Т.А., Хорошевского В.Ф., Романова В.П., Романова А.Н., Одинцова Б.Е., Попова Э.В., Тельнова Ю.Ф. и др.

При проектировании базы знаний советующей системы была поставлена основная цель: сформировать информацию о влиянии внешней среды на региональную социально-экономическую систему [3]. Для этого были опрошены эксперты, результаты их опроса были обработаны в виде соответствующих таблиц. Кроме того, в базе знаний советующей системы находятся классификаторы факторов внешней среды и составляющих региональной социально-экономической системы, разработанные авторами. Важным элементом базы знаний советующей системы является комплекс управленческих мероприятий, нивелирующий или усиливающий влияние внешней среды на региональную систему [1].

На следующем этапе разработки базы знаний советующей системы происходит выделение и графическое представление изучаемых понятий и связей. Так, на основе табличного представления данных экспертов происходит формирование лингвистической переменной ответов экспертов, затем определяется результирующее нечеткое множество ответов экспертов и задается его графическое представление. Отдельным элементом базы знаний системы выступает блок управленческих мероприятий, которые представляются в виде таблицы в соответствии с условиями их применения. Формирование нечетких правил продукции позволяет произвести выбор необходимых управленческих мероприятий на основе разработанной продукционной системы правил [3].

Целевой ориентир информационной советующей системы (ИСС) – это автоматизация обработки анкетных данных экспертиз, формирования по ним статистической отчетности, поддержки принятия решений руководителей и специалистов на основе формирования комплекса управленческих мероприятий. Кроме того, в возможности информационной советующей системы заложено повышение достоверности результатов экспертиз путем увеличения количества экспертов. Следовательно, разработанная информационная советующая система повышает эффективность обработки и анализа экспертных оценок, что в целом обеспечивает эффективное принятие решений руководителями и специалистами.

Модель информационной безопасности разрабатываемой информационной советующей системы

Формирование модели информационной безопасности разрабатываемой информационной советующей системы позволяет определить содержание наиболее актуальных угроз, их объекты и источники. Четкое понимание наиболее возможных угроз позволяет определить способы, направления и средства защиты от них. На рис. 1 представлено графическое изображение модели информационной безопасности программного продукта. В качестве источников угроз безопасности информационной советующей системы могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

При определении угроз безопасности информационной советующей системы оценке подлежат угрозы, связанные со всеми типами источников. Однако в целях создания и эксплуатации адекватной эффективной системы защиты информации в информационной советующей системе

следует в первую очередь уделять внимание оценке антропогенных угроз, связанных с несанкционированными (неправомерными) действиями субъектов по нарушению безопасности (конфиденциальности, целостности, доступности) информации, в том числе с целенаправленными воздействиями программными (программно-техническими) средствами на информационные системы, осуществляемыми для нарушения (прекращения) их функционирования (компьютерные атаки). В процессе определения угроз безопасности информации на всех стадиях (этапах) жизненного цикла разрабатываемой информационной системы необходимо регулярно проводить идентификацию источников угроз.

Для идентификации угроз безопасности информации разрабатываемой информационной советующей системы можно использовать следующий кортеж:

$$T_i = \langle \{I_i\}, \{U_i\}, \{R_i\}, \{O_i\}, \{K_i\} : i \in N \rangle,$$

где T_i - i-я угроза информационной советующей системы; I_i - множество источников i-й угрозы (нарушитель) информационной советующей системы; U_i – множество уязвимостей информационной советующей системы под воздействием i-й угрозы; R_i - множество способов реализации i-й угрозы информационной советующей системы; O_i - множество объектов воздействия i-й угрозы; K_i - множество последствий i-й угрозы.

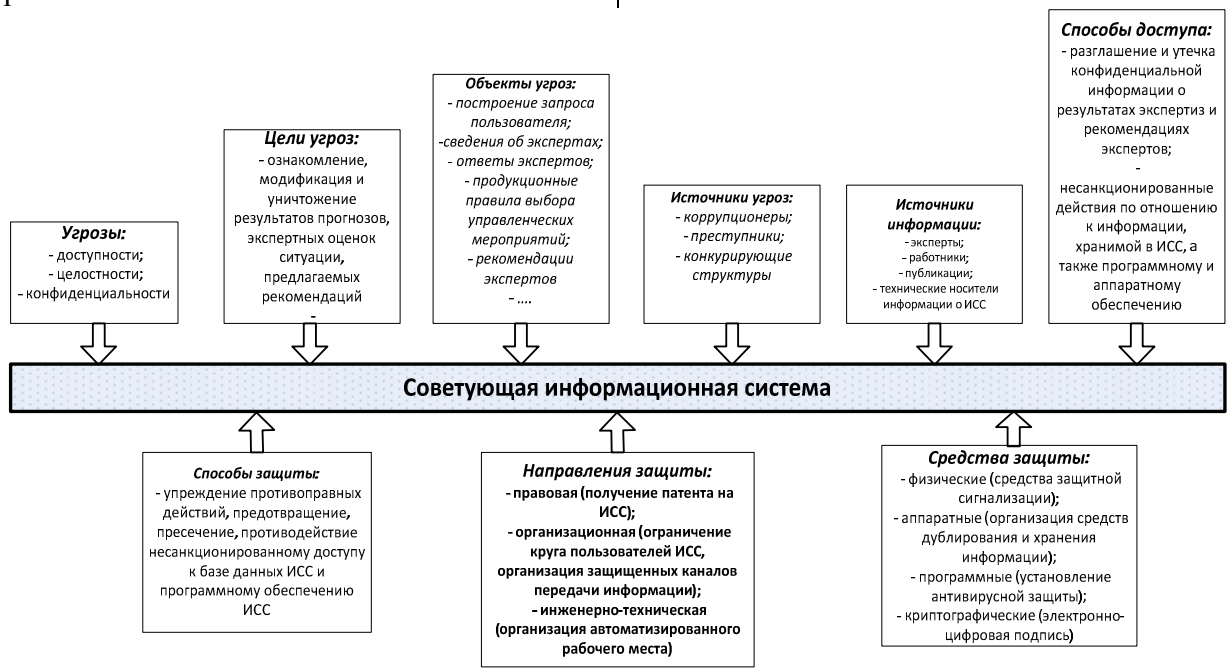

Рис.1. Модель информационной безопасности информационной советующей системы

Идентифицированная угроза безопасности разрабатываемой информационной советующей системы подлежит блокированию, если она является актуальной. Другими словами, определяется вероятность реализации рассматриваемой угрозы нарушителем с соответствующим потенциалом, которая приведет к неприемлемым негативным последствиям для информационной советующей системы. Определим, что

$$для\ \forall T_i\ \exists \{P_i, X_i : i \in N\},$$

где P_i - вероятность реализации i-й угрозы; X_i - степень ущерба от i-й угрозы.

Решение об угрозы безопасности для информационной советующей системы с заданными структурно-функциональными характеристиками и условиями функционирования принимается в соответствии с табл. 1.

Таким образом, угрозы безопасности информации для разрабатываемой информационной советующей системы могут быть оценены как актуальные.

Таблица 1

Актуальность угроз безопасности информационной советующей системы

Вероятность реализации *i*-й угрозы	Степень ущерба от *i*-й угрозы		
	Высокая	Средняя	Низкая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная

В ходе эксплуатации информационной советующей системы планируется регулярно проводить анализ изменения угроз безопасности, а ранее выявленные актуальные угрозы подлежат периодической переоценке. Периодичность переоценки определяется менеджером информационной системы исходя из особенностей ее функционирования (но не реже одного раза в год). По результатам анализа проводится уточнение модели угроз безопасности информационной советующей системы.

Основной угрозой безопасности для разрабатываемой информационной советующей системы будет являться нарушение целостности, доступности и конфиденциальности данных системы. В соответствии с предложенной моделью информационной безопасности под уязвимостями информационной советующей системы будем понимать следующие элементы:

1. В подсистеме ввода данных – ввод экспертных оценок и процедуру построения запроса пользователя.

2. В базе знаний системы – архив оценок экспертов, формализованные сведения о компетенции экспертов, перечень продукционных правил выбора управленческих мероприятий, рекомендации экспертов.

3. В блоке диагностики и вывода данных – классификаторы факторов внешней среды и составляющих региональной социально-экономической системы, процедуры подбора управленческих мероприятий и формирования матриц влияния внешней среды на региональную систему.

4. Программно-технический комплекс (автоматизированные рабочие места, телекоммуникационное оборудование, каналы связи) и программное обеспечение.

Источниками угрозы безопасности разрабатываемой информационной советующей системы будем считать компьютерных злоумышленников, осуществляющих целенаправленное деструктивное воздействие.

С учетом наличия прав доступа и возможностей по доступу к информации и/или компонентам информационной советующей системы выделим два типа нарушителей:

- внешние нарушители – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

- внутренние нарушители – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Наибольшими возможностями по реализации угроз безопасности обладают внутренние нарушители. Таким образом, при оценке их возможностей необходимо учитывать принимаемые организационные меры по допуску к работе в информационной советующей системе. Возможности внутреннего нарушителя зависят от установленного порядка допуска физических лиц к информационной системе и ее компонентам, а также от мер по контролю за доступом и работой этих лиц. В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и/или логический доступ к компонентам информационной системы и/или содержащейся в них информации или не иметь такого доступа.

Анализ прав доступа проводится как минимум в отношении следующих компонентов информационной системы:

- устройств ввода/вывода (отображения) информации;

- беспроводных устройств;

- программных, программно-технических и технических средств обработки информации;

- съемных машинных носителей информации;

- машинных носителей информации, выведенных из эксплуатации;

- активного (коммутационного) и пассивного оборудования каналов связи;

- каналов связи, выходящих за пределы контролируемой зоны.

Уровень реализации угрозы безопасности информационной советующей системы определим как сети, сетевые приложения и сервисы, а также операционные системы. Соответственно, определяя типы объектов, подверженных угрозе безопасности, выделим:

- для сетевого уровня – маршрутизаторы, коммуникаторы и концентраторы;

- уровня сетевых приложений и сервисов – программные компоненты передачи данных по компьютерным сетям;

- уровня операционных систем – файлы данных.

Под обеспечением информационной безопасности в предлагаемой советующей системе будем подразумевать наличие некоторого количества организационно-технических средств, обеспечивающих безопасность любого потенциального канала утечки информации. Барьерами защиты информации в предлагаемой информационной советующей системе выступают механизмы электронной цифровой подписи, протоколы идентификации, стандарт X509, алгоритм Диффи - Хеллмана.

При определении перспективных направлений совершенствования разрабатываемой информационной советующей системы выделим такой существенный недостаток, как трудность в определении всех путей злоумышленных действий по отношению к системе. Следовательно, это ухудшает адекватность предложенной модели информационной безопасности и определяет дальнейшие пути ее совершенствования.

На основе ряда показателей определим текущий уровень проектной защищенности информационной советующей системы [5;6] (табл. 2). Для этого сформулируем структурно-функциональные характеристики информационной советующей системы, условия ее эксплуатации и оценим уровень защищенности по шкале «высокий – средний – низкий».

Таблица 2

Уровень проектной защищенности информационной советующей системы

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	Уровень проектной защищенности информационной системы ($Y_{1П}$)		
	Высокий	Средний	Низкий
1. По структуре информационной системы:			
- автономное автоматизированное рабочее место;	+		
- локальная информационная система;		+	
- распределенная информационная система			+
2. По используемым информационным технологиям:			
- системы на основе виртуализации;			+
- системы, реализующие облачные вычисления;			+
- системы с мобильными устройствами;			+
- системы с технологиями беспроводного доступа;		+	
- грид-системы;			+
- суперкомпьютерные системы			+
3. По архитектуре информационной системы:			
- системы на основе тонкого клиента;	+		
- системы на основе одноранговой сети;		+	
- файл-серверные системы;			+
- центры обработки данных;			+
- системы с удаленным доступом пользователей;			+
- использование разных типов операционных систем (гетерогенность среды);		+	
- использование прикладных программ, независимых от операционных систем;		+	
- использование выделенных каналов связи		+	
4. По наличию (отсутствию) взаимосвязей с иными информационными системами:			
- взаимодействующая с системами;			+
- невзаимодействующая с системами		+	

Окончание табл. 2

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	Уровень проектной защищенности информационной системы ($Y_{1П}$)		
	Высокий	Средний	Низкий
5. По наличию (отсутствию) подключений к сетям связи общего пользования: - подключенная; - подключенная через выделенную инфраструктуру (gov.ru или иную); - неподключенная	+ +	 +	 +
6. По размещению технических средств: - расположенные в пределах одной контролируемой зоны; - расположенные в пределах нескольких контролируемых зон; - расположенные вне контролируемой зоны	+	 +	 +
7. По режимам обработки информации в информационной системе: - многопользовательские; - однопользовательские	 +		 +
8. По режимам разграничения прав доступа: - без разграничения; - с разграничением		 +	 +
9. По режимам разделения функций по управлению информационной системой: - без разделения; - выделение рабочих мест для администрирования в отдельный домен; - использование различных сетевых адресов; - использование выделенных каналов для администрирования		 + + +	 +
10. По подходам к сегментированию информационной системы: - без сегментирования; - с сегментированием		 +	 +

Оценим возможность реализации *i*-й угрозы безопасности информации в зависимости от уровня защищенности информационной системы и потенциала нарушителя (табл. 3).

Таблица 3

Возможность реализации угрозы безопасности информации для разрабатываемой информационной советующей системы

Уровень защищенности / Потенциал нарушителя	Высокий	Средний	Низкий
Базовый (низкий)	Низкая	Средняя	Высокая
Базовый повышенный (средний)	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

Таким образом, для разрабатываемой информационной советующей системы возможность реализации угрозы безопасности информации оценивается как высокая.

Степень возможного ущерба определяется экспертным методом как высокая. Это означает, что в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия для разрабатываемой информационной системы и приостановка ее функционирования.

На основе изложенного построим модель информационной безопасности информационной советующей системы (табл. 4).

Место модуля информационной безопасности в структурно-функциональной схеме информационной советующей системы

Структурно-функциональная модель разработанной информационной советующей системы оценочно-диагностического типа представлена на рис. 2.

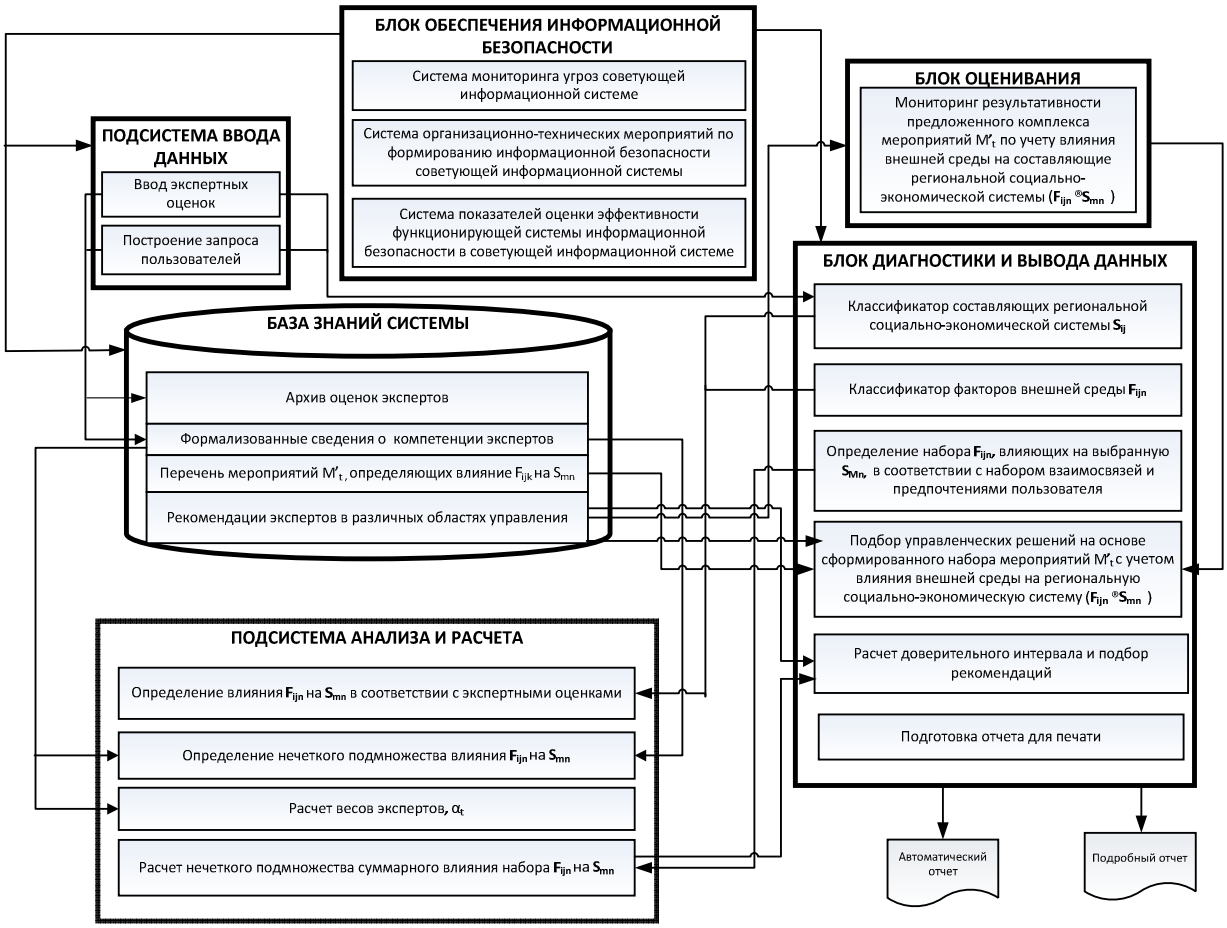

Рис. 2. Структурно-функциональная модель разработанного программного комплекса

Подсистема ввода данных отвечает за корректный ввод оценок экспертов, взаимосвязей и построение запроса пользователем. В оценочном блоке представлены процедуры оценки (мониторинга) результативности предложенного комплекса мероприятий ($M_t^{'}$) по учету влияния факторов внешней среды (F_{ijk}) на составляющие социально-экономической системы региона (S_{mn}). В блоке диагностики и вывода данных формируются классификаторы факторов внешней среды F_{ijk} и составляющих социально-экономической системы региона S_{mn}. Здесь же осуществляется подбор управленческих решений на основе сформированного набора мероприятий ($M_t^{'}$) с учетом влияния внешней среды на региональную систему. Также в блоке диагностического направления представлены таблицы влияния факторов внешней среды (F_{ijk}) на составляющие социально-экономической системы региона (S_{mn}). Там же формируются отчеты для печати.

Таблица 4

Модель информационной безопасности для разрабатываемой информационной советующей системы

Угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
Угрозы утечки по техническим каналам						
Угрозы утечки акустической информации	Высокая	Высокая	Низкая	Актуальная	-	Инструкция пользователя Технологический процесс
Угрозы утечки видовой информации						
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	Высокая	Высокая	Низкая	Актуальная	-	Инструкция пользователя Технологический процесс
Угрозы несанкционированного доступа к информации						
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн						
Кража носителей информации	Высокая	Высокая	Низкая	Актуальная	Охранная сигнализация Хранение в сейфе Шифрование данных при помощи ViPNetSafeDisk	Акт установки средств защиты Учет носителей информации Инструкция пользователя
Кража ключей доступа	Высокая	Высокая	Низкая	Актуальная	Хранение в сейфе	Инструкция пользователя
Кража, модификация, уничтожение информации	Высокая	Высокая	Низкая	Актуальная	Шифрование данных при помощи ViPNetSafeDisk Система защиты от НСДViPNetPersonalFirewall	Акт установки средств защиты
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Высокая	Высокая	Низкая	Актуальная	Шифрование данных при помощи ViPNetSafeDisk	Ремонт в организациях, имеющих лицензию на защиту информации Акт установки средств защиты
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);						
Компьютерные вирусы	Высокая	Высокая	Низкая	Актуальная	Антивирусное ПО «Касперский 6.0»	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите

Окончание табл.4

Угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Высокая	Высокая	Низкая	Актуальная	Настройка средств защиты	-
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также факторов неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера						
Утрата ключей доступа	Высокая	Высокая	Низкая	Актуальная	Хранение в сейфе	Инструкция пользователя Инструкция администратора безопасности Журнал учета паролей
Непреднамеренная модификация (уничтожение) информации сотрудниками	Высокая	Высокая	Низкая	Актуальная	Настройка средств защиты	Резервное копирование Инструкция пользователя
Угрозы преднамеренных действий внутренних нарушителей						
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Высокая	Высокая	Низкая	Актуальная	-	Обязательство о неразглашении Инструкция пользователя
Угрозы несанкционированного доступа по каналам связи						
Несанкционированный доступ через сети международного обмена	Высокая	Высокая	Низкая	Актуальная	Межсетевойэкран ViPNet Firewall	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
Несанкционированный доступ через ЛВС организации	Высокая	Высокая	Низкая	Актуальная	Межсетевой экран ViPNet Firewall	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
Утечка атрибутов доступа	Высокая	Высокая	Низкая	Актуальная	Межсетевой экран ViPNetFirewall Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
Угрозы перехвата при передаче по проводным (кабельным) линиям связи						
Перехват за переделами с контролируемой зоны	Малая	Низкая	Низкая	Неактуальная	Средства криптографической защиты	Технологический процесс

Подсистема анализа и расчета программного комплекса состоит из блока процедур, оценивающих влияние F_{ijk} на S_{mn}, блока определения нечеткого подмножества влияния F_{ijk} на S_{mn}, блока процедур, обеспечивающих расчет весов экспертов α_t, а также блока расчета нечеткого подмножества суммарного влияния F_{ijk} на S_{mn}.

База знаний системы содержит архив оценок экспертов, формализованные сведения о компетенции экспертов, набор мероприятий ($M_t^{'}$), учитывающих влияние F_{ijk} на S_{mn}, а также набор рекомендаций экспертов в различных областях знаний. Заполнение базы знаний, используемой при формировании управленческих решений в информационной советующей системе, будет происходить с помощью опытных экспертов: топ-менеджеров промышленных предприятий, представителей региональной власти разных уровней управления, привлекаемых внешних экспертов-консультантов транснациональных консалтинговых агентств.

Важным элементом информационной советующей системы является блок обеспечения ее информационной безопасности, который представлен системами мониторинга потенциальных угроз, организационно-технических мероприятий по формированию информационной безопасности, а также показателей оценки эффективности функционирования системы информационной безопасности [4]. Функционально этот блок связан с такими элементами информационной советующей системы, как подсистема ввода данных, база знаний системы и блок диагностики и вывода данных.

Результатом работы информационной советующей системы будет являться формирование комплекса управленческих решений, позволяющих повысить качество управления на разных уровнях региональной власти.

СПИСОК ЛИТЕРАТУРЫ

1. Аверченкова, Е.Э. Разработка структурно-функциональной схемы и алгоритмов работы информационной советующей системы по формированию управленческих решений на промышленном предприятии/ Е.Э.Аверченкова, А.В.Аверченков, В.К.Черкасов, Д.В.Аксененко// Вестник Брянского государственного технического университета. - 2015. - № 4 (48). - С.113-120.
2. Аверченкова, Е.Э. Информационный подход к оценке уровня экономической безопасности в региональных социально-экономических системах/ Е.Э.Аверченкова, Н.А.Кулагина// Актуальные проблемы социально-гуманитарных исследований в экономике и управлении: материалы II междунар. науч.-практ. конф. проф.-преподават. состава, магистров и студентов фак. экономики и управления (г.Брянск, 10 дек. 2015 г.): в 2 т. / под ред. Е.И.Сорокиной, Е.А.Дергачевой. - Брянск: БГТУ, 2015. - Т.1. - С.146-152.
3. Аверченкова, Е.Э. Особенности управления региональными социально-экономическими системами на основе нечеткой логики/ Е.Э.Аверченкова, А.В.Аверченков// Экономические системы современной России: теоретические и практические проблемы развития: кол. моногр. / под ред. А.Д.Шафронова, Ю.Н.Каткова. - Брянск: Новый проект, 2015. - С. 35-53.
4. Аверченкова, Е.Э. Построение региональной информационной советующей системы оценочно-диагностического характера/ Е.Э.Аверченкова, А.В.Аверченков, В.К.Черкасов// Вестник славянских вузов. – Тирасполь, 2015. - № 4. - С. 121-127.
5. Бородакий, Ю.В. Метод определения ценности информации для оценивания рисков безопасности информации в автоматизированных системах управления/ Ю.В.Бородакий, Г.В.Куликов, А.В.Непомнящих// Безопасность информационных технологий. - 2005. - № 1. - С. 41-42.
6. Метод построения формальных моделей реализации угроз информационной безопасности автоматизированных систем/ О.Ю.Макаров, В.А.Хвостов, Н.В.Хвостова// Вестник Воронежского государственного технического университета. - 2010. - Т.6. - №11. - С. 22-25.
7. Формальная модель полного множества реализаций угроз информационной безопасности автоматизированных систем/ В.А.Хвостов, М.А.Багаев, А.А.Кисляк// Вестник Воронежского государственного технического университета. - 2011. - Т.7. - № 2. - С. 33-37.

1. Averchenkova, E.E. Development of structural-functional circuit and algorithms of information advising system operation on management solutions-making formation at enterprise/ E.E. Averchenkova, A.V. Averchenkov, V.K. Cherkasov, D.V. Aksenenko// *Bulletin of Bryansk State Technical University*. - 2015. - № 4 (48). - pp. 113-120.
2. Averchenkova, E.E. Information approach to evaluation of economic security level in regional social-economic systems/ E.E. Averchenkova, N.A.Kulagina// *Urgent Problems of Social-Humanitarian Researches in Economy and Management: Proceedings of the II-d Inter. Scientific-Pract. Conf. of Teaching Staff, Masters and Students of the Faculty of Economy and Management (Bryansk, December 10, 2015)*: in 2 Vol. / under the editorship of E.I.Sorokina, E.A.Dergacheva. - Bryansk: BSTU, 2015. - Vol.1. - pp.146-152.
3. Averchenkova, E.E. Peculiarities in regional social-economic systems management based on fuzzy logic/ E.E.Averchenkova, A.V.Averchenkov// *Economic Systems of Modern Economy: Theoretical and Practical Problems of Development*: corporate author / under the editorship of A.D.Shafronov, Yu.N.Katkov. - Bryansk: New project, 2015. - pp. 35-53.
4. Averchenkova, E.E. Formation of regional information advising system of estimating-diagnostic character/ E.E.Averchankova, A.V.Averchenkov, V.K.Cherkasov// *Bulletin of Slavic Colleges. – Tiraspol*, 2015. - № 4. - pp. 121-127.
5. Borodaky, Yu.V. Method for definition of information value to estimate risks of information security in automated systems of management/ Yu.V.Borodaky, G.V.Kulikov, A.V.Nepomnyashchikh// *Information Techniques Safety*. - 2005. - № 1. - pp. 41-42.
6. Method for formal models formation of threats realization to information security of automated systems / O.Yu.Makarov, V.A.Khvostov, N.V.Khvostova// *Bulletin of Voronezh State Technical University*. - 2010. - Vol.6. - №11. - pp. 22-25.
7. Formal model of full set of threat realizations to information security of automated systems / V.A.Khvostov, M.A.Bagaev, A.A.Kislyak// *Bulletin of Voronezh State Technical University*. - Vol.7. - № 2. - pp. 33-37.

Статья поступила в редколлегию 12.04.2016.
Рецензент: д.т.н., профессор Брянского государственного технического университета Аверченков А.В.

Сведения об авторах:

Аверченкова Елена Эдуардовна, к. т. н., доцент кафедры «Экономика, организация производства и управление» Брянского государственного технического университета, тел.: 89038691330, e-mail: lena_ki@inbox.ru.
Гончаров Дмитрий Иванович, студент кафедры «Системы информационной безопасности» Брянского государственного технического университета, e-mail: jeriho32@yandex.ru.
Лысов Дмитрий Андреевич, студент кафедры «Системы информационной безопасности» Брянского государственного технического университета, e-mail: lysov_da@tu-bryansk.ru.

Averchenkova Elena Eduardovna, to. so-called, associate professor "Economy, production organization and management" Bryansk state technical university, ph.: 89038691330, e-mail: lena_ki@inbox.ru.
Goncharov Dmitry Ivanovich, student of Information security systems department of the Bryansk state technical university, e-mail: jeriho32@yandex.ru.
Lysov Dmitry Andreevich, student of Information security systems department of the Bryansk state technical university, e-mail: lysov_da@tu-bryansk.ru.