УДК 004.05

АНАЛИЗ НАПРАВЛЕНИЙ И РЕЗУЛЬТАТОВ МОДЕРНИЗАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ФИРМЫ-ПАРТНЕРА «1С» С ЦЕЛЬЮ ПОВЫШЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ

Статья поступила в редакцию 06.03.2018, в окончательном варианте – 14.06.2018.

Романова Оксана Михайловна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а

Аспирант; ассистент кафедры, e-mail: chobitoksana@mail.ru

Честнов Алексей Александрович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а

студент, e-mail: hydroman7eve@mail.ru

Показана актуальность решения задачи модернизации информационной системы фирмы-партнера «1С» с целью повышения уровня информационной безопасности деятельности организации. Обоснована необходимость подбора методики, позволяющей произвести оценку состава и структуры системы на соответствие требованиям информационной безопасности. Описаны существующие подходы к решению задачи оценки состава и структуры информационной системы фирмы-партнера «1С». К ним относятся методики CRAMM, FRAP, OCTAVE и др. Охарактеризованы достоинства и недостатки этих методик. Представлена свободная от таких недостатков методика оценки уровня информационной безопасности информационной системы, являющаяся частью общей методики оценки качества информационных систем «Ревизор». Приведены основные положения данной методики. Обосновано, что данная методика требует адаптации под особенности информационной системы конкретной организации. Приведены характеристики рассматриваемой организации, существенные для темы статьи. В целях адаптации указанной методики была проанализирована диаграмма потоков данных информационной системы «Обработка заказов клиентов» на примере деятельности организации по ведению нового проекта. Результатом анализа стала ясная демонстрация взаимоотношений информационных процессов на определенном примере. Для проведения адаптации методики к использованию применительно к рассматриваемой организации в соответствии с рекомендациями, приведенными в проекте методики ФСТЭК по определению угроз безопасности информации в информационной системе, была сформирована экспертная комиссия. Она решала такие задачи: определение состава объектов нечеткой когнитивной модели; заполнение базы знаний, описывающей с помощью нечетких продукционных правил влияние повреждений элементов информационной системы на работоспособность сервисов информационной безопасности; формирование входных данных для методики «Ревизор». В частности, экспертами были определены средства защиты информации, угрозы для информационной системы, ее потенциальные уязвимости, виды атак на информационные системы, возможные повреждения. Далее экспертами была произведена оценка непосредственно состава и структуры информационной системы фирмы-партнера «1С»; оценен уровень ее информационной безопасности. Результаты оценивания: текущий уровень информационной системы в организации – «Высокий», событийно-прогнозный уровень информационной безопасности – «Средний», уровень обеспечения сервиса «конфиденциальность» – «Средний» (индекс схожести нечетких чисел 1.0); уровень обеспечения сервиса «целостность» – «Средний» (индекс схожести 0.9); уровень обеспечения сервиса «доступность» – «Средний» (индекс схожести 0.9); уровень обеспечения сервиса «достоверность» – «Средний» (индекс схожести 0.8).Эти оценки послужили основанием для разработки и внедрения рекомендаций по модернизации состава и структуры информационной системы. В частности, было решено использовать следующее: программное обеспечение для создания защищенного внутреннего локального чата; SFTP-сервер с защищенным соединением; выделенный почтовый сервер.

Ключевые слова: информационная система, информационная безопасность, методы оценки, 1С, фирма-партнер, структура рисков, оценки рисков; множество концептов, лингвистическая переменная, нечеткое когнитивное моделирование, методика «Ревизор», модернизация информационной системы

"1C" FIRM PARTNER'S INFORMATION SYSTEM UPGRADE TO INCREASE ORGANIZATION'S INFORMATION SECURITY LEVEL

The article was received by editorial board on 06.03.2018, in the final version – 14.06.2018.

Romanova Oksana M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation

Post-graduate student, Assistant, e-mail: chobitoksana@mail.ru

Chestnov Aleksey A., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation

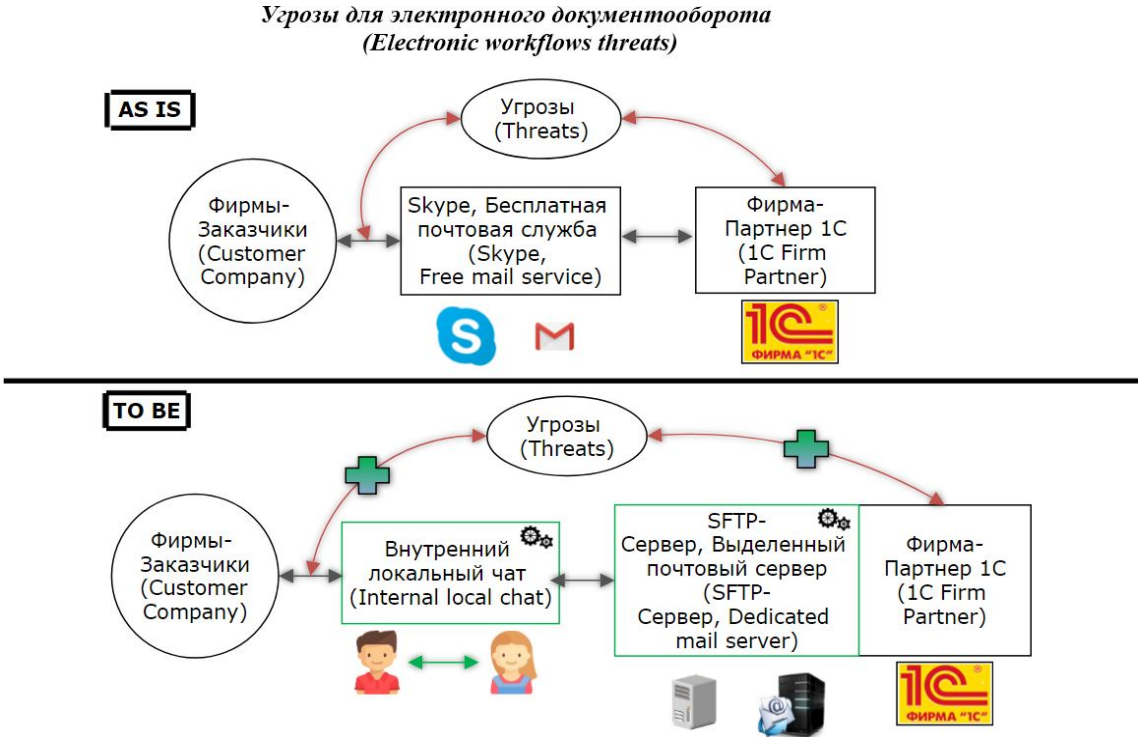
Student, e-mail: hydroman7eve@mail.ru

The article shows the relevance of the solving the task of "1C" firm partner's information system upgrade to increase organization's information security level. The authors substantiated the necessity to choose the method, which allows evaluating the compliance of "1C" firm partner's information system composition and structure with information security requirements. The paper outlines existing approaches for solving the task of evaluating "1C" firm partner's information secu-

rity composition and structure. They include CRAMM, FRAP, OCTAVE methods etc. The authors point out their main advantages and disadvantages. The paper makes a presentation of a method of evaluation of the information security of an information system that is free of the disadvantages. This method is part of general IS quality assessment methodology called "Revizor". The authors describe main strategies of this method. It is reasonable that this method requires adaptation to specific characteristics of organization IS, so the authors dwell on the characteristics of the organization under consideration. To adapt the method the authors analyze the IS data flow diagram titled "Handling of the customers' orders", exemplifying organization's activity on implementation of a new project and showing interrelations of information flows. They organized an expert commission to make adjustments of the method for the implementation for the considered organization to make it compatible with the recommendations cited in FSTEK draft method on defining security threats to information system. This commission solves the following tasks: defining the object composition of fuzzy cognitive models, building a knowledge base that describes the influence of damaged elements of information system on the performance of information security services by employing fuzzy production rules and forming input data for "Revizor" method. In particular, expert commission have defined information security facilities variety, information system's threats variety, information system's vulnerabilities variety, attacks and damage variety. Then experts have evaluated information system composition, structure and level of its information security. They assessed current information security level as "High", event-forecasting level as "Middle", level of confidentiality service provision as "Middle" (commonality index for fuzzy numbers is 1.0), level of integrity service provision as "Middle" (commonality index is 0.9), level of fidelity service provision as "Middle" (commonality index is 0.8). The assessment serves as a basis for developing and implementing recommendations on information system composition and structure modernization. These recommendations have resulted in the following decisions: software for protected inside local chat, SFTP server with secured connection and dedicated mailbox server.

Keywords: information system, information security, evaluation methods, 1C, partner firm, risk structure, risk assessments, concept variety, linguistic variable, fuzzy cognitive modeling, "Revizor" method, information system upgrade

Graphical abstract (Графическая аннотация)



Введение. Фирмы-партнеры (ФП) «1С» – это компании, входящие в партнерскую сеть «1С» и имеющие опыт массового обслуживания пользователей в рамках проекта «1С: Информационно-техноло-гическое сопровождение». В области поставок программ 1С делового назначения есть два основных варианта партнерства – Дилер и Франчайзи. Необходимым условием заключения дилерского договора 1С является согласованная обеими сторонами разовая (закупки в течение месяца) стартовая закупка. Для заключения договора «1С:Франчайзи» необходимыми условиями являются определенные начальные затраты и уплата ежеквартального взноса. Также для своей работы франчайзи необходимо приобрести программный продукт/продукты «1С:Предприятие» и аттестовать в фирме «1С» не менее двух специалистов-внедренцев. При выполнении этих условий фирма-франчайзи получает сертификат и последующую поддержку в работе от фирмы «1С».

Указанные организации оказывают услуги не только по внедрению и сопровождению типовых конфигураций «1С», но и по доработке существующих программных решений под нужды конкретных фирм-заказчиков. При этом в качестве объектов для доработки могут быть выбраны разработки, включенные во всероссийскую корпоративную базу разработок, выполненных различными ФП «1С». Это позволяет ускорить и повысить качество разработок, так как они выполняются не с нуля.

Специфика деятельности ФП «1С» предполагает возможность использования следующих вариантов работы с информацией.

- Применение программ удаленного администрирования для обновления/доработки информационных баз «1С» у заказчиков.
- Хранение и обработку информационных баз «1С» заказчиков в собственной информационной системе ФП.
- Доступ к собственным разработкам ФП (внешние отчеты, печатные формы, обработки, нетиповые конфигурации) большого количества сотрудников.

Таким образом, деятельность ФП «1С» сопряжена с высокими уровнями рисков в сфере информационной безопасности (ИБ). Существует вполне реальная возможность утечки информации, обрабатываемой в ФП; атак на сервера, эксплуатируемых в ФП; кражи интеллектуальной собственности (новые конфигурации, расширения конфигураций, обработки, печатные формы «1С» и пр.). Это, в свою очередь, может повлечь за собой потери денежных средств и репутации не только самой ФП, но и компаний-заказчиков. Поэтому информационные системы (ИС) ФП, используемые для разработки и сопровождения решений фирмы «1С», должны быть организованы таким образом, чтобы обеспечить требуемый уровень ИБ.

Исходя из этого, была сформулирована цель данной работы – подобрать подходящую методику, позволяющую произвести оценку состава и структуры ИС ФП на соответствие требованиям ИБ, предъявляемыми владельцами ФП к ИС организации.

Описание подходов к решению задачи оценки состава модулей и структуры ИС ФП на соответствие требованиям ИБ. Существует несколько подходов к оценке состава модулей и структуры ИС на соответствие требованиям ИБ: оценка рисков информационной безопасности (например, методики CRAMM [1,11], FRAP [2], OCTAVE и т.д.); определение актуальных угроз ИБ (например, «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК [16]. Однако эти методики имеют следующие недостатки: не позволяют сделать вывод о том, что именно нужно изменить в ИС для достижения требуемого уровня ИБ; не учитывают слабую формализуемость процесса оценки уровня ИБ; возможность наличия текущих повреждений ИС (повреждения файлов операционной системы, приложений и пр.), которые могут оказывать усиливающий эффект в отношении величины предполагаемого ущерба от реализации атак на ИС.

От указанных недостатков свободна методика оценки уровня ИБ ИС, являющаяся частью общей методики оценки качества информационных систем «Ревизор», описанной в [4–6]. Предлагаемый авторами настоящей статьи подход к оценке на основе нечеткого когнитивного моделирования позволяет применять указанную методику в организациях различных отраслей, в том числе и в ФП. Однако для этого методика должна быть адаптирована к особенностям этих организаций. В рамках такой адаптации должны быть сформированы элементы множеств концептов нечеткой когнитивной модели (НКМ), применяемой в методике (например, перечень актуальных угроз для ИС, перечень уязвимостей системы); оценены связи между концептами НКМ; заполнены базы знаний, необходимые для оценки текущего уровня ИБИС.

Основные положения методики оценки уровня ИБ. Для решения задачи оценки ИБ в методике «Ревизор» использован аппарат НКМ. Его важнейшим преимуществом являются совместное использование качественных и количественных оценок входных параметров, представленных экспертами; использование неполной, нечеткой и даже противоречивой информации.

Для формализации оценок отдельных критериев ИБ в рассматриваемой методике введена лингвистическая переменная «Уровень фактора» и терм-множество ее значений QL. Оно состоит из девяти элементов, принадлежащих отрицательной и положительной областям оценок: QL = {Высокий отрицательный (B^-); Выше среднего отрицательный (BC^-); Средний отрицательный (C^-); Низкий отрицательный (H^-); Нулевой (0); Низкий положительный (H^+); Средний положительный (C^+); Выше среднего положительный (BC^+); Высокий положительный (B^+)}. В качестве семейства функций принадлежности для QL предложено использовать девятиуровневый классификатор, в котором функциями принадлежности нечетких чисел (НЧ), заданных на отрезке [–1,1] (обозначаемым как R), являются трапеции с такими характеристиками:

$$\{B^-(-1;-1;-0{,}85;-0{,}75);\ BC^-(-0{,}85;-0{,}75;-0{,}65;-0{,}55);C^-(-0{,}65;-0{,}55;-0{,}45;-0{,}35);$$
$$H^-(-0{,}45;-0{,}35;-0{,}25;-0{,}15);«0»(-0{,}25;-0{,}15;0{,}15;0{,}25);\ H^+(0{,}15;\ 0{,}25;0{,}35;0{,}45);$$
$$C^+(0{,}35;0{,}45;0{,}55;0{,}65);\ BC^+(0{,}55;0{,}65;0{,}75;0{,}85);\ B^+(0{,}75;\ 0{,}85;1)\} \quad (1)$$

Здесь в каждом нечётком числе (НЧ) с компонентами a_1, a_2, a_3, a_4 используются такие обозначения: a_1 и a_4 – абсциссы нижнего основания, a_2 и a_3 – абсциссы верхнего основания трапеции. В случае четкого числа $a_1=a_2=a_3=a_4$. Отрицательная часть классификатора используется для нахождения отклонений полученных оценок от требуемых.

Использование данного классификатора является целесообразным, поскольку в соответствии с [17–23] лингвистический анализ на его основе будет непротиворечивым. Классификатор удовлетворяет требованиям «серой» шкалы Поспелова: наличие нейтральной точки посреди интервала неопределенности и монотонное убывание экспертной уверенности в классификации по мере роста «Х». Такому комплексу требований удовлетворяют, разумеется, не только трапециевидные числа. Однако эти числа вы-

ражают ту простую идею, что если нет никаких дополнительных соображений о характере убывания экспертной уверенности, то линейный вид соответствующей функции принадлежности наиболее рациональный (экономичный) – cv/ http://www.ifel.ru/content/docs/an_books/Book4.pdf.

В целях разработки комплексного критерия оценки качества ССОД, отражающего многокритериальность целевого показателя была использована схема по рисунку 1.

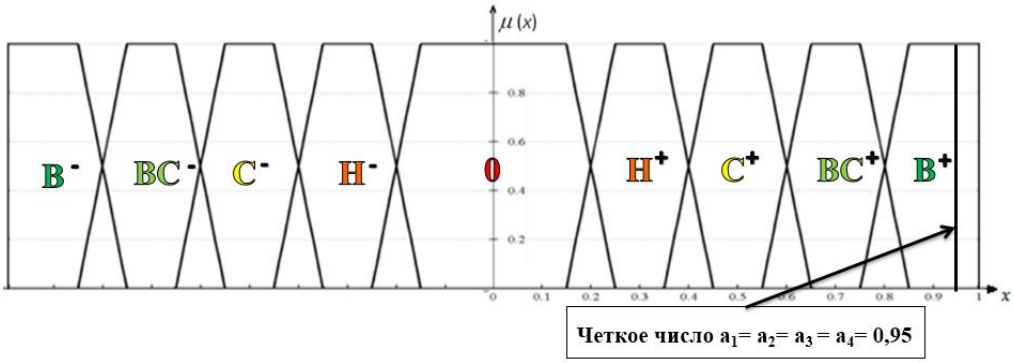


Рисунок 1 – Формализация вербальных оценок – Лингвистическая переменная «Уровень фактора»

Комплексный критерий оценки качества – Quality:

$$Quality = \alpha_1 \cdot Safety + \alpha_2 \cdot Effect + \alpha_3 \cdot Inv(Cost) + \alpha_4 \cdot Sec + \alpha_5 \cdot Adap + \alpha_6 \cdot Int + \\ + \alpha_7 \cdot Con + \alpha_8 \cdot Inv(Com) + \alpha_9 \cdot Str + \alpha_{10} \cdot Lab + \alpha_{11} \cdot Div + \alpha_{12} \cdot Suit + \alpha_{13} \cdot IS, \quad (2)$$

где соответственно – коэффициенты влияния надежности (Safety), социально-экономического эффекта (Effect), затрат на владение (Cost), безопасности для персонала (Sec), адаптивности (Adap), интегрируемости (Int), целостности (Con), сложности (Com), структурированности (Str), лабильности (Lab), делимости (Div), валидности (Suit), информационной безопасности (IS) ССОД на уровень качества (Quality).

Сама методика оценки уровня ИБ имеет различные этапы в зависимости от стадии жизненного цикла ИС. Для проектируемых ИС необходимо вычислить событийно-прогнозный уровень ИБ, который демонстрирует последствия от реализации потенциальных угроз в отношении ИС. Для уже эксплуатируемых ИС необходимо сначала вычислить текущий уровень ИБ, который показывает влияние текущих повреждений системы на уровень ИБ. Затем, после внедрения (реализации) мер по ликвидации текущих повреждений ИС, вычисляется событийно-прогнозный уровень ИБ.

В основе методики оценки событийно-прогнозного уровня ИБ лежит нечеткая когнитивная модель, структура которой представляет кортеж [12]:

$$<ID, G, L, S, Al, \Omega>, \quad (3)$$

где ID – исходные данные для оценки уровня ИБ ИС; G – ориентированный граф, не содержащий горизонтальных ребер в пределах одного уровня иерархии; L – лингвистическая переменная, формализующая качественные (вербальные) оценки каждого фактора в графе G; S – множество весов ребер графа G, отражающих степень влияния концептов на заданный элемент следующего уровня иерархии; Al – алгоритм для вычисления значений концептов на каждом из уровней иерархии G; Ω – индекс схожести, позволяющий лингвистически распознавать результаты вычислений с нечеткими числами. Граф G нечеткой когнитивной модели приведен на рисунке 2.

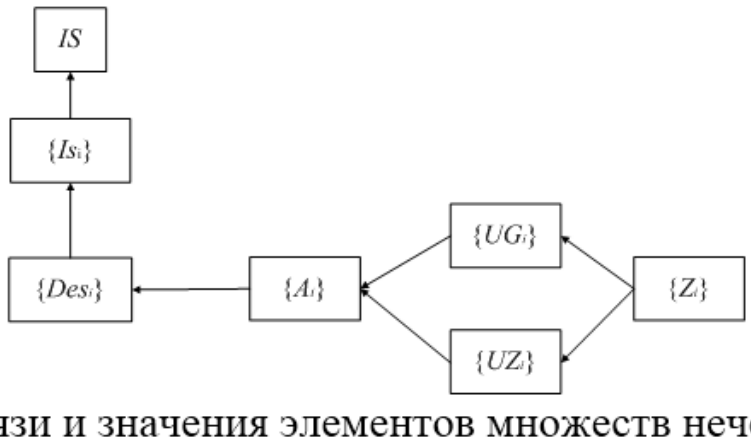


Рисунок 2 – Граф G нечеткой когнитивной модели оценки ИБ

На вершине графа находится комплексный критерий ИБ *IS*. Информационная безопасность определяется способностью ИС обеспечивать сервисы ИБ $\boldsymbol{Is}_{\{1,2,3,\ldots\}}$. Второй слой (уровень, ступень) графа *G* представлен повреждениями элементов системы $\boldsymbol{Des}_{\{1,2,3,\ldots\}}$, которые образуются в результате атак на информационные активы $\boldsymbol{A}_{\{1,2,3,\ldots\}}$. Атаки являются результатом реализации угроз для ИС $UG_{\{1,2,3,\ldots\}}$ через уязвимости ИС $\boldsymbol{UZ}_{\{1,2,3,\ldots\}}$. Последний уровень графа *G* представлен средствами защиты информации (СЗИ) $\boldsymbol{Z}_{\{1,2,3,\ldots\}}$.

Алгоритм оценки событийно-прогнозного уровня ИБ ИС, используемый в методике «Ревизор», имеет следующий вид [13]:

1. *Оценка уровня средств и мер защиты информации.*
2. *Вычисление уровня уязвимостей.*
3. *Вычисление уровня опасности угроз.*
4. *Вычисление уровня «разрушительности» атак.*
5. *Вычисление уровня повреждений элементов ИС и СЗИ.*
6. *Вычисление уровня информационной безопасности.*

Данные правила называются *атомарными.*

Алгоритм оценки текущего уровня ИБ включает в себя следующие этапы: 1) оценка уровня текущих повреждений на каждом уровне иерархии (рис. 3); 2) поиск соответствующих атомарных правил в базе знаний; 3) оценка состояния результирующего показателя на текущем уровне иерархии согласно найденным правилам; 4) идентификация блоков, содержащих узловые повреждения. Под *узловыми* понимаются блоки, повреждения которых при достижении определенного (*критического*) уровня не позволяют идентифицировать повреждения некоторых блоков на следующем уровне иерархии (такие блоки на рисунке 4 имеют исходящие стрелки), уровень которых выше критического и исключение из рассмотрения вышестоящих блоков, повреждения которых в связи с этим не могут быть определены; 5) вычисление интегральной оценки для каждого из результирующих показателей. Исключение из рассмотрения тех блоков, повреждения которых невозможно определить, не снижает адекватность оценки. Причина – в этом случае интегральная оценка результирующего показателя определяется критическим уровнем соответствующего узлового повреждения.

Стоит отметить, что иерархия повреждений была построена таким образом, чтобы охватить все уровни ИСФП (аппаратные средства обработки данных; программную среду; файлы, непосредственно хранящие важную информацию) и направления защиты информации. При этом каждый блок может быть декомпозирован для повышения точности оценки для конкретного объекта информатизации.

Рисунок 3 – Иерархия возможных повреждений ИС ФП

Для оценки результирующих показателей на каждом уровне иерархии повреждений используется процедура применения *атомарных* правил. На основании оценок повреждений на рассматриваемом уровне иерархии осуществляется поиск соответствующих «атомарных» правил в базе знаний и путем построения *блоковых* правил определяется влияние повреждений каждого блока иерархии на результирующие показатели:

$$K_j^k : Если \left(\&_{i=1}^{W}\left[Des_i = \overline{D_i}\right]\right)$$

$$mo\,(\&_{j=1}^{M}[\max_m\{O_m\}_{m\in\{\arg(\min_i(\bar{s}))\}}(K_j^k = \min_i(\overline{S_i}))]), \qquad (4)$$

где k – номер блока иерархии; K_j^k – j-ый сервис безопасности, характеризующий k-ый блок; W – количество повреждений в k-м блоке; $\overline{D_i}$ – уровень наблюдаемых повреждений Des_i; M – количество сервисов ИБ, на которые влияют повреждения k-го блока; $\overline{S_i}$ – определяемое согласно соответствующему *атомарному* правилу значение K_j при уровне повреждения Des_i равного $\overline{D_i}$; O_m – степень уверенности эксперта в оценке влияния повреждения Des_i, имеющего уровень $\overline{D_i}$, на j-ый сервис безопасности.

Интегральная оценка сервисов ИБ K_j определяется как минимум значений критериев ИБ, найденных на каждом из уровней иерархии повреждений, которые удалось идентифицировать.

Адаптация методики «Ревизор» для оценки уровня ИБ фирмы-партнера «1С». Рассмотрим адаптацию методики «Ревизор» для оценки уровня ИБ на примере ИС «Обработка заказов клиентов» (рис. 4–5) ведущей фирмы-партнера «1С» в г. Астрахани ООО ПКФ «Бест софт». Основными направлениями деятельности компании являются следующие:

1) продажа, доставка, установка, настройка программных продуктов фирмы «1С»;
2) сопровождение программных продуктов фирмы «1С»;
3) проведение тренинг-семинаров с клиентами;
4) обучение клиентов работе в программах серии «1С»;
5) комплексные отраслевые проектные внедрения – выпуск тиражных программных продуктов «1С»;
6) подбор необходимого программного обеспечения для заказчиков;
7) постановка управленческого учета и бюджетирования на предприятиях;
8) внедрение прикладных решений семейства «1С: Предприятие 8»;
9) разработка и внедрение сложных конфигураций для автоматизации уникальных и специфических бизнес-процессов предприятий;
10) сопровождение прикладных решений и сложных конфигураций;
11) автоматизация предприятий энергетической сферы на базе программных продуктов «1С: Энергетика».

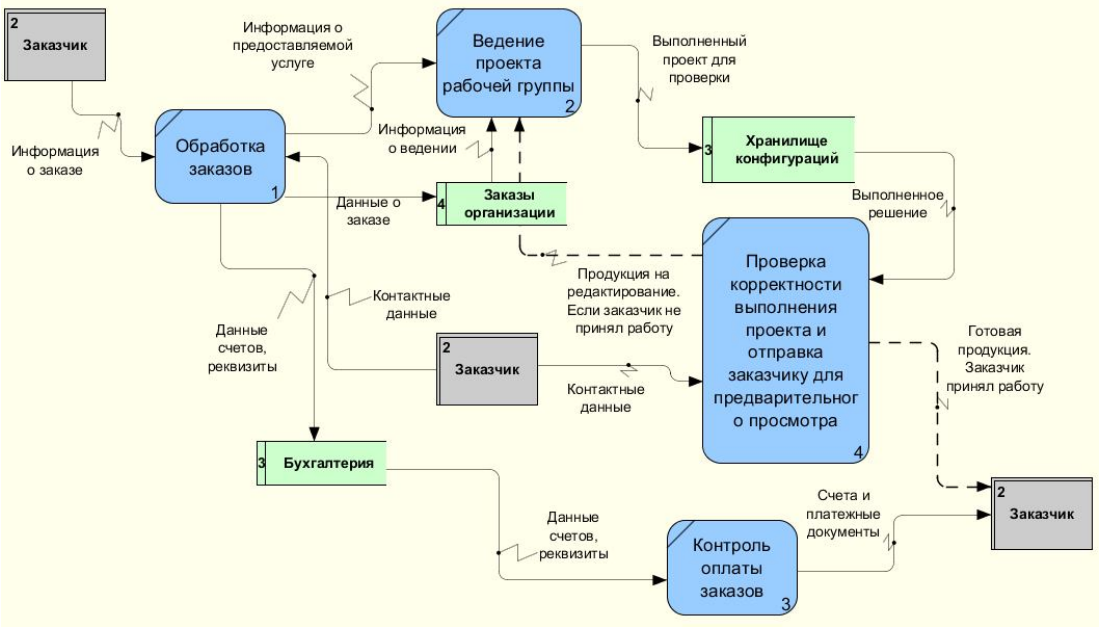


Рисунок 4 – Диаграмма потоков данных ИС «Обработка заказов клиентов» на примере деятельности по ведению нового проекта

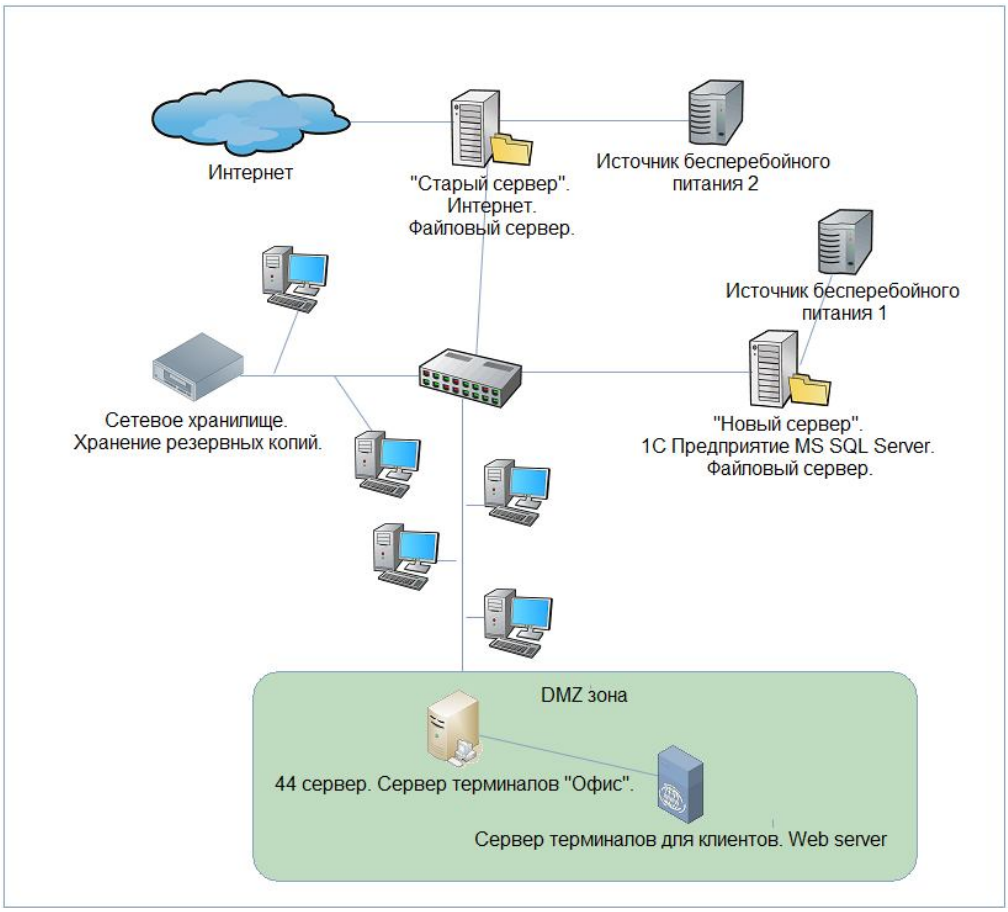


Рисунок 5 – Структура ЛВС описываемой организации

Для проведения адаптации методики «Ревизор» в соответствии с рекомендациями, приведенными в проекте методики ФСТЭК по определению угроз безопасности информации в ИС [16], была сформирована экспертная комиссия. В нее вошли сотрудники отдела разработки ООО ПКФ «Бест софт» в количестве двух человек; руководителя отдела сопровождения; технического директора фирмы.

Основные задачи, которые были поставлены перед комиссией: определение состава элементов НКМ; заполнение базы знаний; формирование входных данных для методики «Ревизор». Обсуждение тем длилось до принятия экспертами согласованного решения, а именно порядка 3.5 часа.

В частности, экспертами было определено множество: средств защиты информации, угроз ИС, уязвимостей ИС, атак ИС, множество повреждений ИС. За основу списков были взяты множества, приведенные в [4]. Эксперты дополнили их следующими элементами, соответствующими особенностям предметной области:

Множество средств защиты информации:

- Z_{31} – меры по обнаружению (предотвращению) вторжений;
- Z_{32} – меры по ограничению программной среды;
- Z_{33} – меры по антивирусной защите рабочих станций;
- Z_{34} – меры по выявлению инцидентов информационной безопасности и реагированию на них;
- Z_{35} – проведение лекционных занятий с персоналом ООО ПКФ «Бест софт».

Множество угроз ИС:

- UG_{33} – угроза изменения компонентов системы;
- UG_{34} – угроза искажения вводимой и выводимой на периферийные устройства информации;
- UG_{35} – угроза некорректного использования функционала программного обеспечения;
- UG_{36} – угроза несанкционированного восстановления удаленной защищаемой информации;
- UG_{37} – угроза несанкционированного копирования защищаемой информации КЕМ;
- UG_{38} – угроза распространения «почтовых червей» в локальной сети фирмы;
- UG_{39} – угроза фишинга в отношении рабочего персонала фирмы;
- UG_{40} – преднамеренное или неумышленное разглашение информации ограниченного доступа;

Множество уязвимостей ИС:

• UZ_{32} – недостатки механизмов разграничения доступаинформационной системы фирмы;

• UZ_{33} – старение и размагничивание носителей информации (дискет и съемных носителей информации, жестких дисков, кабелей, соединительных линий);

• UZ_{34} – неисправности программного обеспечения (ОС и СУБД, прикладных программ, сервисных программ, антивирусных программ).

Множество атак ИС:

• A_{34} – изменение компонентов системы;

• A_{35} – искажение вводимой и выводимой на периферийные устройства информации;

• A_{36} – некорректное (но санкционированное) использование функционала программного обеспечения;

• A_{37} – несанкционированное восстановление удаленной защищаемой информации;

• A_{38} – несанкционированное копирование защищаемой информации;

• A_{39} – распространение «почтовых червей»;

• A_{40} – фишинг.

Итоговые количества элементов множеств: для средств защиты информации – 37, угроз ИС – 40, уязвимостей ИС – 34, атак ИС – 40.

Далее экспертами была произведена непосредственно оценка состава и структуры ИС ФП на соответствие требованиям ИБ. Сначала был оценен текущий уровень ИБ как «Высокий». В связи с этим эксперты сразу перешли к оценке событийно-прогнозного уровня ИБ. Его значение было вычислено по формулам (4)–(9) и определено как «Средний» (индекс схожести равен 1,0): уровень конфиденциальности – «Средний» (индекс схожести равен 1,0); уровень целостности – «Средний» (индекс схожести равен 0,9); уровень доступности – «Средний» (индекс схожести равен 0,9); уровень достоверности – «Средний» (индекс схожести равен 0,8).

Полученная оценка послужила основанием для разработки и внедрения рекомендаций по модернизации состава и структуры ИС.

М1) В частности было решено использовать программное обеспечение для создания защищенного внутреннего локального чата. Данная мера предложена с целью прекращения использования бесплатных небезопасных аналогов (например, Skype и др.). Их применение для крупных ИТ-компаний считается небезопасным с точки зрения конфиденциальности. Подобное решение предложено с целью закрыть имеющиеся уязвимости ИС организации (UZ_{20} – ненадёжность внешних коммуникационных каналов и др.). Использование группового чата в пределах локальной сети для корпоративного общения имеет ряд достоинств: автономность работы при отсутствии подключения к сети Интернет; исключение вероятности коллизий при выходе из строя одного или нескольких узлов; возможность безопасного сетевого общения [13, 14]. В рамках реализации предложения была составлена сравнительная таблица (табл. 1), описывающая преимущества и недостатки предлагаемых средств для создания защищенного внутреннего локального чата.

Таблица 1 – Преимущества и недостатки предлагаемых средств для создания защищенного внутреннего локального чата

Наименование решения	**Преимущества**	**Недостатки**
Microsoft Teams Classic Client	Индивидуальная настройка и расширение, встроенные приложения Office 365, возможность создания закрытых чатов для групп пользователей, возможность назначения ролей и разрешений для участников группы, качественный аудит и журналирование событий работы системы MicrosoftGraph, возможность создания и редактирования документов прямо в приложении	Ошибки интерфейса: настройка группового чата, визуальная составляющая, ошибки отображения сообщений в чатах ввиду большого количества встроенных приложений
CommFort	Улучшенный интерфейс выбора получателей, возможность настроить размеры элементов интерфейса, списков пользователей, отключение подчиненным отображения информации об активности руководителей, демонстрация экрана	Ошибки с отображением медиаконтента, сбои при передаче файлов в групповом чате, некорректное отображение журналов событий
MyChat	Быстрый обмен сообщениями, файлами, отправка SMS – сообщений, возможность создания групповых чатов с распределением ролей для пользователей, облегченный язык разметки, возможность аудио и видеосвязи, наличие электронной доски объявлений	Графический интерфейс на сервере, нет возможности объединять сервера, ОС до Windows 2000 не поддерживаются

Итоговый выбор продукта был сделан на основе нескольких ключевых критериев (возможностей):

1) возможность создания закрытых групп пользователей, сотрудничающих для выполнения поставленных задач (беседы, файлы и заметки в каналах видимы только участникам закрытой группы);

2) назначение ролей и разрешений для участников группы;

3) отслеживание качества звонков и качества обслуживания, аудит и ведение отчетов;

4) наличие голосовых сообщений и видеозвонков.

В результате было предложено использовать Microsoft Teams Classic Client для ОС Windows.

М2) Было решено использовать SFTP-сервер с защищенным соединением. Данная мера предложена с целью закрыть имеющиеся уязвимости ИС организации (UZ_9 – возможность хищения носителей информации,UZ_{10} – возможность копирования информации,UZ_{32} – преднамеренное или неумышленное разглашение информации ограниченного доступа и др.). SFTP-сервер имеет ряд явных преимуществ таких, как поддержка беспарольной аутентификации с помощью SSH-ключей (пароль пользователя не хранится на диске компьютера и нет необходимости вводить его вручную) [10]. Данное изменение в структуре ИС предприятия обезопасит пользователей системы от кейлогеров, отслеживающих и запоминающих введенные с клавиатуры данные, которые могли попасть в систему в результате действий персонала фирмы, а также клиентов (в случае аппаратных клавиатурных шпионов). Также к числу преимуществ данного решения необходимо отнести поддержку символических ссылок и более стабильное, быстрое соединение. Основным назначением нововведения является контроль доступа пользователей к определенным каталогам и файлам вместе с возможностью осуществлять только разрешенные действия над содержимым SFTP-хранилища. В рамках реализации предложения была построена сравнительная таблица (табл. 2), описывающая преимущества и недостатки предлагаемых SFTP – серверов с защищенным соединением.

Таблица 2 – Преимущества и недостатки предлагаемых SFTP–серверов с защищенным соединением

Наименование решения	**Преимущества**	**Недостатки**
Bitvise SSH Server	Легкий интерфейс, неограниченное количество соединений, ведений журнала и статистики, высокая производительность и скорость, поддержка виртуальной файловой системы, настройка скорости загрузки файлов может быть сконфигурирована для каждого пользователя или группы пользователей отдельно	Отсутствует поддержка виртуальных аккаунтов, что ограничивает создание большого количества аккаунтов Windows
Cerberus FTP Server	Удобный интерфейс, использование FTP, SFTP, FTPS, SCP протоколов, а также протоколы аутентификации LDAP, DB	Отсутствует балансировка нагрузки
ProFTPD	Удобный CLI и GUI интерфейс, использование FTP, SFTP, FTPS протоколов, а также протоколы аутентификации DB	Отсутствует балансировка нагрузки. Ограниченное количество соединений. Несовместимость с ОС Windows

В результате было предложено использовать Bitvise SSH Server для ОС Windows.

Выбор данного продукта был сделан на основе нескольких ключевых критериев:

1) тип операционной системы рабочих станций, установленных в организации;

2) возможность контроля пропускной способности и скорости загрузки для каждого пользователя или группы пользователей;

3) простота настройки с помощью BssCfg и PowerShell через текстовый файл, скрипт или визуально-удобную командную строку.

М3) Было решено настроить и использовать выделенный почтовый сервер. Данная мера была введена с целью закрыть имеющиеся угрозы ИС организации (UG_{11} – угроза заражения компьютера вредоносным программным обеспечением и др.). Использование бесплатных почтовых сервисов крупными ИТ-компаниями небезопасно с точки зрения конфиденциальности. Использование выделенного почтового сервера имеет ряд достоинств: отсутствие сбоев в работе системы, гарантия целостности хранимых данных, возможность резервного копирования, наличие средств мониторинга деятельности пользователей и контроль доступа [9]. Входящая и исходящая почта хранится на собственном сервере организации, а не на бесплатных серверах. Это гарантирует, что данные не будут анализироваться третьими лицами, и даёт полную независимость от поставщика облачных почтовых услуг. А использование резервных копий предотвратит потерю важной информации. Сравнительная таблица 3 описывает преимущества и недостатки предлагаемых выделенных почтовых серверов.

Таблица 3 – Преимущества и недостатки предлагаемых на рынке выделенных почтовых серверов

Наименование решения	Преимущества	Недостатки
hMailServer	Наличие антиспама, встроенная антивирусная поддержка, подписи домена и аккаунтов, поддержка нескольких механизмов антиспама: «Черный» список хостов DNS (DNSBL), «Черный» список ссылок DNS (SURBL), «Серый» список, структура политики отправителя, поддержка ОС Windows	Отсутствие встроенного фильтра, ошибки русификации продукта
Courier Mail Server	Система фильтрации maildrop	Доступ к полному функционалу открывается лишь в комбинации с серверами Qmail, Exim и Postfix

В рамках работы было предложено использовать hMailServer для ОС Windows.

Выбор данного продукта был сделан на основе нескольких ключевых критериев:

1) тип операционной системы рабочих станций, установленных в организации.

2) авторизация пользователей через локальную систему.

3) поддержка возможности защиты от спама.

Повторная экспертная оценка показала, что реализация данных мер позволила повысить уровень ИБ до уровня «Высокий».

Выводы.1. Охарактеризована специфика работы компаний-партнеров «1С», и доказана актуальность организации и совершенствования структуры и состава их ИС. 2. Описаны существующие подходы к решению задачи оценки состава и структуры ИС ФП на соответствие требованиям ИБ, приведены их ключевые недостатки. 3. Доказано, что предлагаемая методика, являющаяся частью общей методики оценки качества ИС «Ревизор», свободна от вышеописанных недостатков. 4. Была проведена адаптация методики «Ревизор» для оценки уровня ИБ ФП «1С». Процесс адаптации рассмотрен на примере ИС «Обработка заказов клиентов» ведущей фирмы-партнера «1С» Астрахани ООО ПКФ «Бест софт». В связи с этим описаны основные направления и особенности деятельности компании. 5. Для проведения оценок ИБ ИС была сформирована экспертная комиссия из числа персонала указанной фирмы. 6. В ходе экспертной оценки членами экспертной комиссии были определены множества: средств защиты информации, угроз ИС, уязвимостей ИС, атак ИС, повреждений ИС. **7**. На основе определенных множеств концептов была произведена оценка состава и структуры ИС ФП на соответствие требованиям ИБ. Полученная оценка послужила основанием для разработки и внедрения рекомендаций по модернизации состава и структуры ИС. В частности, использование программного обеспечения для создания защищенного внутреннего локального чата, использование SFTP-сервера с защищенным соединением; использование выделенного почтового сервера. Предложенные меры позволили повысить уровень ИБ ИС рассматриваемой организации.

Список литературы

1. Ажмухамедов И. М. Оценка состояния защищенности данных организации в условиях возможности реализации угроз информационной безопасности / И. М. Ажмухамедов, О. М. Князева // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 3. – С. 24–39 (http://hi-tech.asu.edu.ru/files/3(31)/24-39.pdf).

2. Ажмухамедов И. М. Формирование у студентов системного подхода к выбору средств защиты информации / И. М. Ажмухамедов, А. Н. Марьенков // Информационное противодействие угрозам терроризма. – 2015. – Т. 2, № 25. – С. 9–13.

3. Анфилов А. С. Системный анализ показателей, связанных с оценкой и управлением ИТ-инфраструктурой организации / А. С. Анфилов, Ю. М. Брумштейн, М. В. Иванова // Прикаспийский журнал: управление и высокие технологии. – 2011. – № 2 (14). – С. 25–32 (http://hi-tech.asu.edu.ru/files/2(14)/25-32.pdf).

4. Асанов А. А. Влияние надежности человеческой информации на результаты применения методов принятия решений / А. А. Асанов, О. И. Ларичев // Автоматика и телемеханика. – 1999. – № 5. – С. 20–31.

5. Баранова Е. К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности / Е. К. Баранова // Управление риском. – 2009. – № 1 (49). – С. 24–31.

6. Баранова Е. К. Методики анализа и оценки рисков информационной безопасности / Е. К. Баранова // Образовательные ресурсы и технологии. – 2015. – № 1 (9). – С. 73–79.

7. Брумштейн Ю. М. Использование информационных технологий и информационная безопасность корпоративных информационных систем медучреждений / Ю. М. Брумштейн, С. В. Чернов, М. Е. Королев // Теория, методы проектирования, программно-техническая платформа корпоративных информационных систем : материалы VII Междунар. науч.-практ. конф., г. Новочеркасск, 25 мая, 2009 г. – Новочеркасск : Юж-Рос. гос. техн. ун-т, 2009. – С. 47–50.

8. Выборнова О. Н. Нечеткий когнитивный подход к оценке рисков / О. Н. Выборнова, И. М. Ажмухамедов // Математические методы в технике и технологиях. – 2015. – № 3 (73). – С. 114–117.

9. Гильдебрандт Р. Postfix. Подробное руководство : пер. с англ. / Р. Гильдебрандт, П. Кеттер. – СПб : Символ Плюс, 2008. – 512 с.

10. Желязны Д. Говори на языке диаграмм : пособие по визуальным коммуникациям для руководителей : пер. с англ. / Д. Желязны. – Москва : Институт комплексных стратегических исследований, 2004. – 220 с.

11. Князева О. М. Управление качеством информационных систем на основе процессного подхода / О. М. Князева // Прикаспийский журнал: управление и высокие технологии. – 2016. – № 2. – С. 36–47 (http://hi-tech.asu.edu.ru/files/2(34)/36-47.pdf).

12. Князева О. М. Нечеткая когнитивная модель процесса оценки качества информационных систем / О. М. Князева // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности : сб. ст. II Всерос. науч.-техн. конф. молодых ученых, аспирантов и студентов. – Таганрог : Южный федеральный университет, 2016. – С. 21–24.

13. Князева О. М. Комплексная оценка качества информационных систем на основе нечеткого когнитивного моделирования / О. М. Князева // Математические методы в технике и технологиях – ММТТ–29: сб. трудов XXIX Междунар. науч. конф. – 2016. – Т. 1. – С. 117–123.

14. Князева О. М. Оценка состояния защищенности данных организации в условиях возможности реализации угроз информационной безопасности / О. М. Князева // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 3. – С. 24–39 (http://hi-tech.asu.edu.ru/files/3(31)/24-39.pdf).

15. Мащенко П. Л. Корпоративные средства внутренних коммуникаций / П. Л. Мащенко, М. О. Пилипенко. – Режим доступа: https://3minut.ru/images/PDF/2017/32/korporativnye-sredstva.pdf//, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.03.2018).

16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – Утв. Заместителем директора ФСТЭК России 15 февраля 2008 г. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380, свободный. – Заглавие с экрана. – Яз. рус.

17. Недосекин А. О. Методологические основы моделирования финансовой деятельности с использованием нечетко-множественных описаний : автореф. дис. док. эконом. наук. – Санкт-Петербург, 2003. – 280 с.

18. Недосекин А. О. Нечетко-множественный анализ риска фондовых инвестиций / А. О. Недосекин // Интернет-вестник ВолгГАСУ. Сер. Строит. информатика. – 2013. – Вып. 10 (30). – Режим доступа: www.vestnik.vgasu.ru, свободный. – Заглавие с экрана. – Яз. рус.

19. Недосекин А. О. Оценка риска бизнеса на основе нечетких данных / А. О. Недосекин. – 2011. – Режим доступа: http:/sedok.narod.ru/index.html, свободный. – Заглавие с экрана. – Яз. рус.

20. Недосекин А. О. Применение нечетких моделей в экономическом анализе / А. О. Недосекин. – 2011. – Режим доступа: http:/sedok.narod.ru/index.html, свободный. – Заглавие с экрана. – Яз. рус.

21. Недосекин А. О. Применение теории нечетких множеств к задачам управления финансами / А. О. Недосекин // Аудит и финансовый анализ. – 2000. – № 2. – Режим доступа: http://www.cfin.ru, свободный. – Заглавие с экрана. – Яз. рус.

22. Недосекин А. О. Финансовый менеджмент на нечетких множествах / А. О. Недосекин. – 2003. – Режим доступа: http:/sedok.narod.ru/index.html, свободный. – Заглавие с экрана. – Яз. рус.

23. Недосекин А. О. Применение теории нечетких множеств к финансовому анализу предприятий / А. О. Недосекин, О. Б. Максимов. – 1999. – Режим доступа: http://www.vmgroup.sp.ru, свободный. – Заглавие с экрана. – Яз. рус.

24. Обзор методик анализа рисков информационной безопасности информационной системы предприятия // CYBERLENINKA. – Режим доступа: https://cyberleninka.ru/article/v/obzor-metodik-analiza-riskov-informatsionnoy-bezopasnosti-informatsionnoy-sistemy-predpriyatiya, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.03.2018).

25. Панфилов К. Vc.ru / К. Панфилов // Инструменты для обращения внутри компании: опыт стартапов с «трибуны». – 11.08.2014. – Режим доступа: https://vc.ru/p/communicate/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.03.2018).

26. Рассел Джесси. Сервер (программное обеспечение) / Джесси Рассел. – Москва : Книга по Требованию, 2012. – 114 с.

27. OCTAVE // CERT. – Available at: http//www.cert.org/resilience/products-services/octave/index.cfm, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.03.2018).

References

1. Azhmukhamedov A. I., Knyazeva O. M. Otsenka sostoyaniya zashchishchennosti dannykh organizatsii v usloviyakh vozmozhnosti realizatsii ugroz informatsionnoy bezopasnosti [Assessment of status for data security of organization in conditions of realization possibility for information security threats]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2015, no. 3 (31), pp. 24–39 (http://hi-tech.asu.edu.ru/files/3(31)/24-39.pdf).

2. Azhmukhamedov A. I., Marenkov A. N. Formirovanie u studentov sistemnogo podkhoda k vyboru sredstv zashchity informatsii [Forming system approach to the choice of information security tools for students]. *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information Counteraction to Threats of Terrorism], 2015, no. 2, pp. 9–13.

3. Anfilov A. S., Brumshteyn Yu. M., Ivanova M. V. Sistemnyy analiz pokazateley, svyazannykh s otsenkoy i upravleniem IT-infrastrukturoy organizatsii [System analysis of indicators related to the assessment and management of the organization's IT infrastructure]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2011, no. 2 (14), pp. 25–32 (http://hi-tech.asu.edu.ru/files/2(14)/25-32.pdf).

4. Asanov A. A., Larichev O. I. Vliyanie nadezhnosti chelovecheskojy informatsii na rezultaty primeneniya metodov prinyatiya resheniy [The influence of the reliability of human information on the results of the application of decision-making methods]. *Avtomatika i telemekhanika* [Automation and Telemechanics], 1999, no. 5, pp. 20–31.

5. Baranova Ye. K. Metodiki i programmnoe obespechenie dlya otsenki riskov v sfere informatsionnoy bezopasnosti [Methods and software for risk assessment in the field of information security]. *Upravlenie riskom* [Risk Management], 2009, no. 1 (49), pp. 24–31.

6. Baranova Ye. K. Metodiki analiza i otsenki riskov informatsionnoy bezopasnosti [Methods of analysis and risk assessment of information security].*Obrazovatelnye resursy i tekhnologii* [Educational Resources and Technologies], 2015, no. 1(9), pp. 73–79.

7. Brumshteyn Yu. M., Chernov S. V., Korolev M. Ye. Ispolzovanie informatsionnykh tekhnologiy i informatsionnaya bezopasnost korporativnykh informatsionnykh sistem meduchrezhdeniy [Use of information technologies and information security of corporate information systems of medical institutions]. *Teoriya, metody proektirovaniya, programmno-tekhnicheskaya platforma korporativnykh informatsionnykh system : materialy VII Mezhdunar. nauch.-prakt. konf., g. Novocherkassk, 25 maya* [Theory, Design Methods, Software and Hardware Platform of Corporate Information Systems. Proceedings of the VII International Scientific and Practical Conference, Novocherkassk, May 25], 2009, no. 1, pp. 47–50.

8. Vybornova O. N., Azhmukhamedov I. M. Nechetkiy kognitivnyy podkhod k otsenke riskov [Fuzzy cognitive approach to risk assessment]. *Matematicheskie metody v tekhnike i tekhnologiyakh* [Mathematical Methods in Engineering and Technology], 2015, no. 3 (73), pp. 114–117.

9. Gildebrandt R., Ketter P. *Postfix. Podrobnoe rukovodstvo* [Postfix. A detailed guide], Saint Petersburg, Simvol Plyus Publ., 2008. 512 p.

10. Zhelyazny D. *Govori na yazyke diagram : posobie po vizualnym kommunikatsiyam dlya rukovoditeley* [Speak in the Language of Diagrams. Manual on Visual Communications for Managers], Moscow, Institute for Comprehensive Strategic Studies Publ. House, 2004. 220 p.

11. Knyazeva O. M. Upravlenie kachestvom informatsionnykh sistem na osnove protsessnogo podkhoda [Quality management of information systems based on the process approach]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2016, no. 2, pp. 36–47 (http://hi-tech.asu.edu.ru/files/2(34)/36-47.pdf).

12. Knyazeva O. M. Nechetkaya kognitivnaya model protsessa otsenki kachestva informatsionnykh system [Fuzzy cognitive model of the process of assessing the quality of information systems]. *Fundamentalnye i prikladnye aspekty kompyuternykh tekhnologiy i informatsionnoy bezopasnosti: sbornik statey II Vserossiyskoy nauchno-tekhnicheskoy konferentsii molodykh uchenykh, aspirantov i studentov* [Fundamental and Applied Aspects of Computer Technology and Information Security. Proceedings of the II All-Russian Scientific and Technical Conference of Young Scientists, Post-Graduate Students and Students], Taganrog, Southern Federal University Publ. House, 2016, no. 1, pp. 21–24.

13. Knyazeva O. M. Kompleksnaya otsenka kachestva informatsionnykh sistem na osnove nechetkogo kognitivnogo modelirovaniya [Complex assessment of the quality of information systems based on odd cognitive modeling]. *Matematicheskie metody v tekhnike i tekhnologiyakh – MMTT–*29 *: sb. tr. XXIX Mezhdunar. nauch. konf.* [Mathematical Methods in Engineering and Technology – MMTT–29. Proceedings of the XXIX International Scientific Conference], 2016, no. 1, pp. 117–123.

14. Knyazeva O. M. Otsenka sostoyaniya zashchishchennosti dannykh organizatsii v usloviyakh vozmozhnosti realizatsii ugroz informatsionnoy bezopasnosti [Evaluation of the state of security of the organization's data in the context of the possible implementation of information security threats]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2015, no. 3, pp. 24–39 (http://hi-tech.asu.edu.ru/files/3(31)/24-39.pdf).

15. Mashchenko P. L., Pilipenko M. O. Korporativnye sredstva vnutrennikh kommunikatsiy [Corporate means of internal communications]. Available at: https://3minut.ru/images/PDF/2017/32/korporativnye-sredstva.pdf (accessed: 22.03.2018).

16. Metodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh [Method of determining actual threats to the security of personal data when processing them in personal information systems]. Approved Deputy Director of FSTEC of Russia on February 15, 2008. Available at: http://fstec.ru//component/attachment/download/290 (accessed: 22.03.2018).

17. Nedosekin A. O. *Metodologicheskie osnovy modelirovaniya finansovoy deyatelnosti s ispolzovaniem nechetko-mnozhestvennykh opisaniy* [Methodological bases of modeling financial activities using fuzzy-multiple descriptions], Saint Petersburg, 2003. 280 p.

18. Nedosekin A. O. Nechetko-mnozhestvennyy analiz riska fondovykh investitsiy [Fuzzy-multiple risk analysis of equity investments]. *Internet-vestnik VolgGASU. Ser. Stroit. informatika* [Internet-Bulletin of VolgGASU. Ser. Building Computer Science], 2013, issue 10 (30). Available at: http:/sedok.narod.ru/index.html (accessed: 22.03.2018).

19. Nedosekin A. O. *Otsenka riska biznesa na osnove nechetkikh dannykh* [Business risk assessment based on fuzzy data]. Available at: http:/sedok.narod.ru/index.html (accessed: 22.03.2018).

20. Nedosekin A. O. *Primenenie nechetkikh modeley v ekonomicheskom analize* [The application of fuzzy models in economic analysis], 2011. Available at: http:/sedok.narod.ru/index.html.

21. Nedosekin A. O. Primenenie teorii nechetkikh mnozhestv k zadacham upravleniya finansami [Application of the theory of fuzzy sets to financial management tasks]. *Audit i finansovyy analiz* [Audit and Financial Analysis], 2000. Available at: http://www.cfin.ru (accessed 22.03.2018)

22. Nedosekin A. O. Finansovyy menedzhment na nechetkikh mnozhestvakh [Financial management on fuzzy sets], 2003. Available at: http:/sedok.narod.ru/index.html (accessed: 22.03.2018).

23. Nedosekin A. O., Maksimov O. B. *Primenenie teorii nechetkikh mnozhestv k finansovomu analizu predpriyatiy* [Application of the theory of fuzzy sets to the financial analysis of enterprises], 1999. Available at: http://www.vmgroup.sp.ru (accessed: 22.03.2018).

24. Obzor metodik analiza riskov informatsionnoy bezopasnosti informatsionnoy sistemy predpriyatiya [Review of methods for analyzing the risks of information security of the enterprise's information system]. *CYBERLENINKA*. Available at: https://cyberleninka.ru/article/v/obzor-metodik-analiza-riskov-informatsionnoy-bezopasnosti-informatsionnoy-sistemy-predpriyatiya (accessed: 22.03.2018).

25. Panfilov K. Vc.ru. *Instrumenty dlya obrashcheniya vnutri kompanii: opyt startapov s «tribuny»* [Tools for internal circulation: the experience of start-ups from the "rostrum"]. Available at: https://vc.ru/p/communicate (accessed: 22.03.2018).

26. Rassel Dzhessi. *Server (programmnoe obespechenie)* [Software], Moscow, Kniga po trebovaniyu Publ., 2012. 114 p.

27. OCTAVE. *CERT*. Available at: http//www.cert.org/resilience/products-services/octave/index.cfm (accessed: 22.03.2018).