DOI: 10.15514/ISPRAS-2021-33(5)-3

Онтологическое обеспечение управления рисками информационной безопасности

И. Бубакар, ORCID: 0000-0003-1094-8666 <Ibbatoure10@gmail.com>
М.Б. Будько, ORCID: 0000-0001-7054-5709 <mbbudko@itmo.ru>
М.Ю. Будько, ORCID: 0000-0002-1444-277X <mbudko@itmo.ru>
А.В. Гирик, ORCID: 0000-0002-4021-7605 <avg@itmo.ru>
Университет ИТМО,
197101, Россия, Санкт-Петербург, Кронверкский пр., д. 49, лит. А

Аннотация. В итоге выполнения работы, ориентированной на повышение эффективности системы информационной безопасности за счет разработки онтологической модели и подхода на ее основе к обеспечению управления рисками информационной безопасности (ИБ), был получен гибкий результат, который призван обеспечить повышение эффективности системы защиты информации за счет снижения временных затрат на принятие управленческих решений. В конце работы проведен сравнительный анализ существующих подходов и методик к управлению рисками ИБ и описываемый подход. На основе разработанной онтологии и подхода на её основе могут быть созданы высокоинтеллектуальные системы управления рисками ИБ и системой защиты информации в целом.

Ключевые слова: информационный риск; управление рисками; защита информации; информационная безопасность; принятие управленческих решений; поддержка принятия решений; динамическая экспертная система; онтология

Для цитирования: Бубакар И., Будько М.Б., Будько М.Ю., Гирик А.В. Онтологическое обеспечение управления рисками информационной безопасности. Труды ИСП РАН, том 33, вып. 5, 2021 г., стр. 41-64. DOI: 10.15514/ISPRAS–2021–33(5)–3.

Ontological support of information security risk management

I. Boubacar, ORCID: 0000-0003-1094-8666 <Ibbatoure10@gmail.com>
M.B. Budko, ORCID: 0000-0001-7054-5709 <mbbudko@itmo.ru>
M.Yu. Budko, ORCID: 0000-0002-1444-277X <mbudko@itmo.ru>
A.V. Guirik, ORCID: 0000-0002-4021-7605 <avg@itmo.ru>
ITMO University,
49, bldg. A, Kronverksky Pr., St. Petersburg, Russia, 197101

Abstract. As a result of the work focused on improving the efficiency of the information security system through the development of an ontological model and an approach based on it to ensure information security (IS) risk management, a flexible result was obtained, which is designed to ensure an increase in the efficiency of the information security system by reducing the time spent on managerial decision-making. At the end of the work, a comparative analysis of existing approaches and techniques to information security risk management and the described approach was carried out. Based on the developed ontology and approach, highly intelligent information security risk management systems and the information security system can be created on its basis.

Keywords: information risk; risk management; information security; information safety; management decision-making; decision support; dynamic expert system; ontology

For citation: Boubacar I., Budko M.B., Budko M.Yu., Guirik A.V. Ontological support of information security risk management. Trudy ISP RAN/Proc. ISP RAS, vol. 33, issue 5, 2021, pp. 41-64 (in Russian). DOI: 10.15514/ISPRAS–2021–33(5)–3

1. Введение

Информационная безопасность (ИБ) является одним из важнейших процессов любой серьёзной современной организации. Поэтому строжайший контроль над ИБ и управление ею в режиме реального времени являются экзистенциональной необходимостью для современной организации. Сегодня ядром ИБ являются анализ и управление информационными рисками (ИР). Поэтому изучение, создание и внедрение средств, автоматизирующих процесс анализа и управления ИР, являются весьма актуальными задачами для любого специалиста в области ИБ. Ведь это позволяет здорово сократить время на принятие управленческих решений (ПУР).

Одним из актуальнейших и многообещающих направлений при решении проблемы автоматизации процессов анализа и управления, как ИР, так и ИБ в целом является применение экспертных систем (ЭС) поддержки принятия решений (ППР), позволяющих выполнить львиную долю функций и рутинных операций, выполняемых обычно персоналом, что сильно сократит время на принятие правильных необходимых управленческих решений. В условиях, когда высокая: динамика изменения требований по ИБ, динамика изменения методологических подходов к ИБ, динамика изменения мнений экспертов по ИБ, динамика изменения факторов, влияющих на информацию, логичным и оправданным является применение динамических экспертных систем (ДЭС). Но имплементация систем управления ИБ на базе ДЭС ППР затруднена нехваткой научно обоснованного методического и методологического аппарата, учитывающего не только требования и специфику управления ИБ, в том числе мнение экспертов компании, но и важную специфику реализации инфраструктуры информационных технологий (ИТ).

ДЭС это, прежде всего, системы, основанные на экспертных знаниях в предметной области (ПрО). В настоящее время, для формализации ПрО используются онтологии. А динамика изменения требований, методологических подходов, мнений экспертов, влияющих на информацию факторов и т.д., можно просто рассматривать как обучение онтологии. Обучить онтологию означает просто корректировать в ней знания или дополнить её новыми знаниями. Сегодня мы знаем, что процесс обучения онтологии может быть полностью автоматизирован различными техниками (правилами вывода, машинным обучением, прецедентным подходом и т.д. и т.п.). Следовательно, можем рассматривать ДЭС, основанные на онтологию, т.е. онтологические ДЭС (ОДЭС). Выше сказанное и определило нашу тему и гипотезу.

Предполагается, что создание онтологии ПрО «Управление рисками ИБ» является очень важным шагом к построению эффективной интеллектуальной системы анализа и управления рисками ИБ. С помощью онтологии можно до мельчайших подробностей объяснить машине смысл понятия и указать его правильное использование. Онтология может содержать все знания ПрО, в том числе аксиомы и правила логического вывода. Как только мы сумели объяснить, по-настоящему онтологическим подходом, машине что такое «ресурс», «ценность ресурса», «угроза», «уязвимость», «вероятность успешной реализации угрозы», «коэффициент разрушительности», «негативное событие», «частота возникновения неблагоприятного события за фиксированный промежуток времени», «риск», «управление рисками» и т.д., то система на основе онтологии будет способна без колебаний обнаруживать негативные события, уязвимости, угрозы, определить риски, дать рекомендации и т.д. Конечно, все зависит от степени разработанности и качества этой самой онтологии. Тогда распознавания проблем ИБ будет основываться на знаниях и правилах логического вывода. Правила позволят извлечь даже сложные имплицитные (не явные) знания, что в свою очередь позволит не включить в онтологию выводимые знания, т.е. сокращать объём работы и сильно оптимизировать как саму онтологию, так и процедуру распознавания уязвимостей, угроз и

т.д. на её основе. Отсюда наша гипотеза о том, что полная и непротиворечивая онтология ПрО «Управление рисками ИБ» с соответствующими правилами логического вывода, в том числе с учетом прецедентов является необходимым и достаточным фундаментом эффективной интеллектуальной системы управления рисками. Отсюда цели и задачи данной работы.

Объектом данной работы является система управления рисками ИБ. **Предметом** работы является онтологическое обеспечение системы управления рисками ИБ. **Целью** является повышение качества и обоснованности принимаемых решений при управлении рисками ИБ за счет организации интеллектуальной ППР на основе онтологии ПрО «Управление рисками ИБ», включающей экспертные знания (стандарты, правовые нормы, концепты, процессы, отношения, требования и ограничения, решающие правила, формулы, алгоритмы, прецеденты и т.д.) и рассуждений по ним.

Для достижения указанной цели требуется решение следующих задач.

1) Составление онтологической модели ПрО «Управление рисками ИБ».
2) Составление онтологической модели процесса управлении рисками ИБ.
3) Определение места и роли управления рисками ИБ на основе ОДЭС ППР.
4) Управление рисками ИБ на основе ОДЭС ППР.
5) Структура подхода на основе ОДЭС ППР.
6) Оценка эффективности СЗИ на основе ОДЭС ППР.

Данная работа является важной составной частью большой исследовательской работы, целью которой является разработка, реализация и исследование современной интеллектуальной системы поддержки ПУР по ИБ с применением подхода онтологического инжиниринга, которая бы учитывала требования и ограничения нормативно правовой документации по ИБ, мнения экспертов по ИБ и связи процессов ИБ, и которая бы обеспечила повышение эффективности системы защиты информации (СЗИ) за счет сокращения временных затрат на ПУР.

2. Онтологическое моделирование предметной области «Управление рисками ИБ»

2.1 Онтология ПрО «Управление рисками ИБ»

2.1.1 Основные концепты ПрО

Из анализа нормативно-правовой базы [1]-[29] была выявлена совокупность базовых концептов ПрО. Ниже перечислены некоторые концепты этой совокупности.

Актив – любая ценность организации. Есть следующие виды активов: материальные активы (например, оборудование), финансовые активы, информационные активы (ИА), человеческие активы (люди и их квалификация, навыки и опыт), процессы, нематериальные активы (например, репутация, имидж). **Информационные активы (ИА)** – информационные ресурсы, в том числе различные виды информации, циркулирующие в информационной системе на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение), или средства обработки информации.

Атака – попытка реализации угрозы (уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования. **Угроза ИБ** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения ИБ. **Угроза** – потенциальная возможность использования уязвимости. **Интенсивность угрозы** – потенциальный ущерб, который может быть нанесен организации в случае реализации данной угрозы. **Уязвимость** – недостаток в

активе или в СЗИ, используя который, можно намеренно нарушить её целостность и вызвать неправильную работу. **Негативное событие (НС)** – событие, которое может породить угрозы ресурсам (активам), задействованным в основных процессах организации.

Основной процесс (ОП) – это совокупность взаимосвязанных мероприятий или задач, направленных на создание определённого продукта или услуги для потребителей. Процесс – агрегированный актив, который оперирует всеми другими активами для достижения бизнес целей организации. **Подпроцесс (ПП)** – процессы, работы, входящие в состав основного процесса и представляющие собой также процессы.

Риск ИБ – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации. **Информационный риск** – это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий. **Приемлемый риск** – такой риск, с которым лицо, принимающее решения (ЛПР), в имеющейся ситуации может смириться. **Толерантный риск** – предельный уровень риска, который организация может выдержать без значительного ущерба для своей финансовой и конкурентной позиции.

Стратегия защиты от угроз - это общая, рассчитанная на перспективу руководящая установка при организации и обеспечении ИБ, направленная на то, достигались цели ИБ при наиболее рациональном расходовании имеющихся ресурсов.

Эффективность средства – оценка, которая отражает, с какой вероятностью применение данного средства локализует соответствующую ему базовую угрозу.

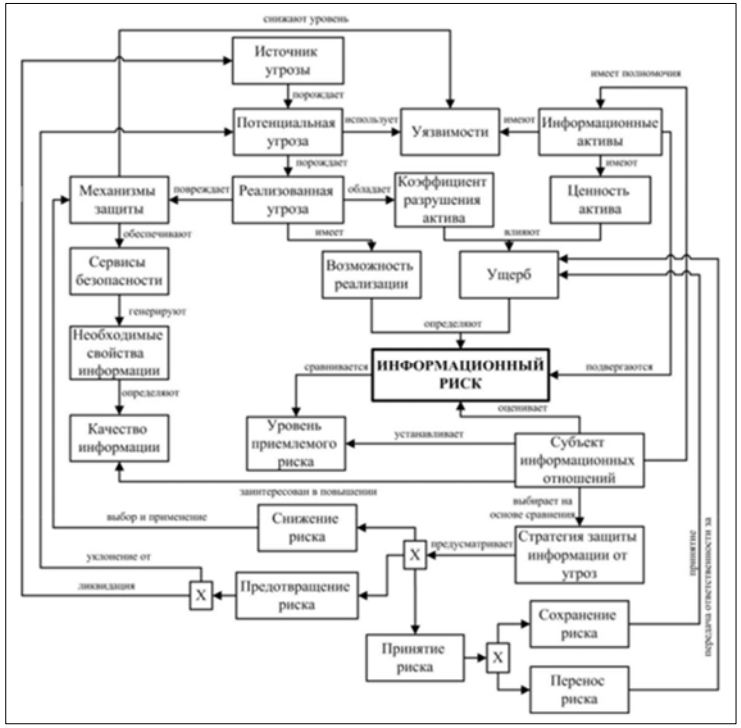

Рис. 1. Онтологическая модель ПрО «Управление рисками ИБ»
Fig. 1. Ontological model of subject area «IS Risk Management»

2.1.2 Онтологическая модель ПрО

На рис. 1 отображена онтологическая модель ПрО «Управление рисками ИБ».

Данная онтологическая модель отражает взаимосвязь основных концептов и компонент управления рисками комплексной системы ИБ.

2.1.3 Характеристики некоторых концептов онтологии ПрО

На рис. 2 и 3 представлены в виде ER-диаграмм свойства, ограничения и взаимоотношения некоторых концептов онтологии ПрО.

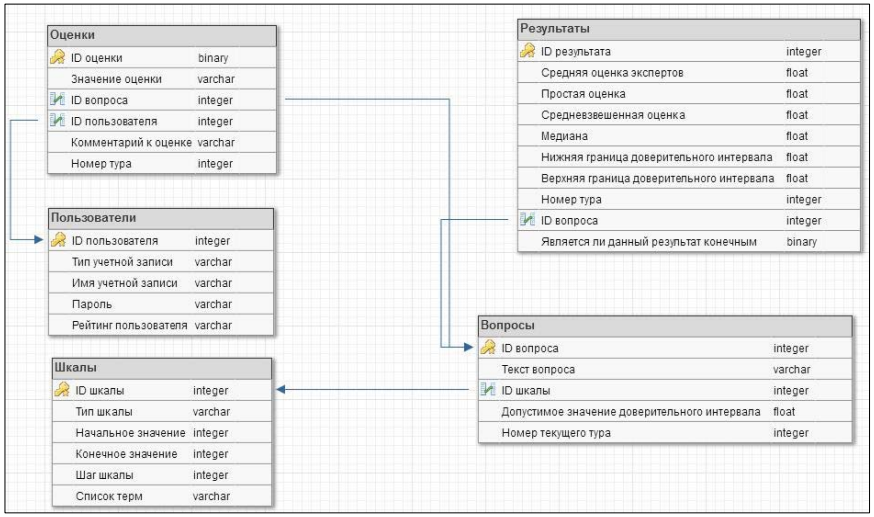

Рис. 2. Характеристики понятия: Вопрос, Шкала, Оценка, Пользователь, Результат
Fig. 2. Characteristics of the concept: Question, Scale, Assessment, User, Result

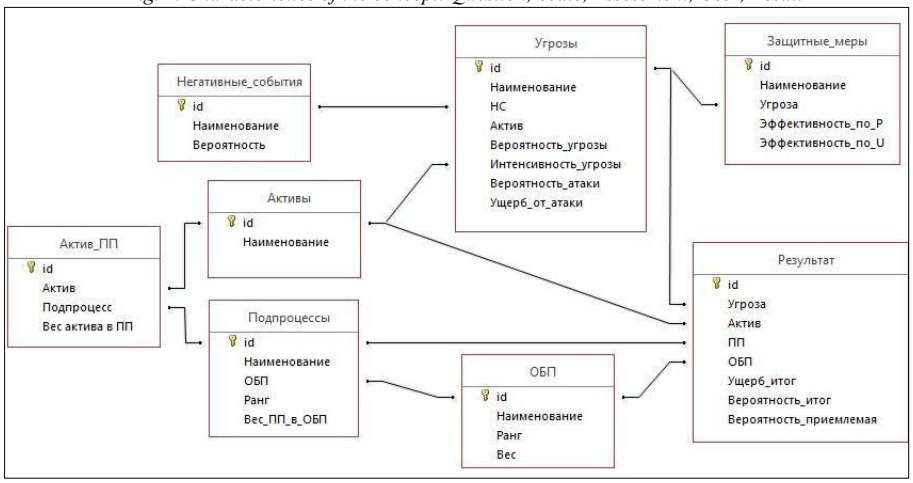

Рис. 3. Характеристики понятия: Актив, Угроза, Негативное событие, Защитная мера, Основной базовый процесс, Подпроцесс, Результат
Fig. 3. Characteristics of the concept: Asset, Threat, Negative event, Protective measure, Main basic process, Sub-process, Result

Характеристики концептов на диаграммах (рис. 2 и рис. 3) представлены в таком виде только для удобства чтения и понятности. Они на самом деле описывают экземпляры классов соответствующих концептов онтологии и являются частью ее.

2.1.4 Возможные вопросы (запросы) к онтологии ПрО

Запросы к онтологии осуществляются для извлечения явных и неявных знаний из неё. В данной работе онтология представлена спецификациями IDEF. В будущем для извлечения больше выгоды из нее, она будет реализована спецификациями и средствами семантического веба. При реализации онтологии спецификациями (RDF/RDFS, OWL, SKOS, FOAF, DC, vCard и т.д.) и средствами (protègè и его плагинами, графами знаний и т.д.) семантического веба, то запросы для извлечения явных знаний могут быть описаны с помощью языка запросов SPARQL, а для извлечения неявных (скрытых) знаний, с помощью правил логического вывода, можно применить языки SHACL, PIN, SWRL и подобные.

Ниже дана вербальная формулировка примеров возможных вопросов (запросов) к онтологии ПрО.

- Является ли данное событие негативным событием?
- Каковы негативные последствия данного негативного события?
- Какие угрозы вызывает данное событие?
- Какие уязвимости может эксплуатировать данная угроза?
- Какие уязвимости присутствуют в системе?
- Какие угрозы присутствуют в системе?
- Каково происхождение угрозы?
- Какие совместимые меры и средства защиты оптимально выбрать для данной угрозы?
- Какие совместимые меры и средства защиты оптимально выбрать для данного набора угроз?
- Совместимы ли данные мера и средство защиты?
- Решают ли данную угрозу данные мера и средство защиты?
- По каким параметрам оптимально выбирать совместимые мера и средство защиты для данной угрозы или их набора?
- Отвечают ли данные мера и средство защиты требованиям данного российского или международного стандарта?
- Отвечают ли данные мера и средство защиты требованиям данной НПД?
- Какова приемлемость данного риска?

2.2 Онтологическая модель процесса управления рисками ИБ

Онтология данного процесса базируется на двух главных понятиях: просчет рисков и обработка рисков. С этими понятиями связаны следующие важные понятия: угрозы ИБ; ИА (объекты воздействия); источники угроз; воздействия на объекты защиты.

При просчете рисков определяются: опасность угрозы; вероятность реализации угрозы; уязвимости реализации угрозы; способы реализации угрозы; возможные разрушительные воздействия; риски и их характеристики.

При обработке рисков должны быть определены корректирующие и предупреждающие воздействия.

3. Управление рисками на основе ОДЭС ППР

3.1 Место и роль управления рисками ИБ на основе ОДЭС ППР

В состав функций данного метода входят: онтологическая формализация требований и систематизация процессов обеспечения ИБ; онтологическая автоматизация совместимого выбора мер защиты и технических средств защиты; логический вывод (мониторинг) действия принятых мер и средств защиты; аналитическое обеспечение деятельности персонала по ИБ.

В результате реализации данного метода мы получим: онтологическую систематизацию требований по управлению ИБ, исходя из состава процессов обеспечения ИБ; связанное применение организационных мер и технических СЗИ; формированную аналитическую базу проведения исследований и анализа состояния ИБ; рационально обоснованное стратегическое, тактическое и оперативное управление процессами обеспечения ИБ; возможности своевременного применения корректирующих и предупреждающих воздействий на основе комплексного анализа состояния ИБ в целом, и объектов защиты в частности; возможности обеспечения планирования развития и поддержания СЗИ; онтологическую формализацию основных и второстепенных процессных составляющих управления и обеспечения ИБ; повышение общего уровня ИБ за счет формализации и систематизации ее основных процессов; снижение операционных рисков за счет уменьшения вероятности реализации угроз ИБ, ввиду повышения ее общего уровня; повышение прозрачности процессов ИБ в рамках СЗИ; повышение оперативности при решении задач обеспечения ИБ; снижение трудоемкости операций по обеспечению ИБ; повышение уровня компетенции персонала организации и специалистов по ЗИ в вопросах ИБ; повышение оперативности реагирования на инциденты ИБ; минимизацию затрат на эксплуатацию СЗИ.

3.2 Управление рисками ИБ на основе ОДЭС ППР

3.2.1 Трудность ПУР при управлении ИБ

Пусть у нас имеется организация, в которой выполняются $i = 1, \dots, n$ равноценных процессов управления ИБ и пусть r_i некоторое количество ресурсов, затрачиваемое на реализацию i-го процесса.

Пусть процесс i характеризуется параметрами: $t_i(r_i)$ – время на получение информации в ходе выполнение процесса с использованием ресурса r_i; (x_i) – количество получаемой информации в ходе выполнения процесса.

Пусть на организацию провели атаку, угрожающую ее непрерывную работу и руководству нужно срочно ПУР для нейтрализации атаки за время t_{max}, при неизменном общем количестве ресурсов R. Тогда: $R = \sum_{i=1}^{n} r_i = const$, и руководству необходимо получить такое количество информации f от всех процессов управления ИБ для перевода СЗИ в безопасное от атаки состояние на основе доступных ресурсов и за не более чем максимальное доступное время на принятие решения. Формально математически это значит:

$$\begin{cases} \sum_{i=1}^{n} f_i(x_i) \rightarrow \max\limits_{x=(x_1,\cdots,x_n)\in Z_+^n} \\ \sum_{i=1}^{n} t_i(r_i)x_i \le t_{max} \end{cases} \quad (1)$$

По теории управления, решение, которое необходимо принять, будет описываться параметрами: F – совокупный объем информации, необходимый для принятия решения; T – время, необходимое для принятия решения и обработки информации; R – состав ресурсов на

выполнение задачи; аналитические алгоритмы для обработки информации и принятия решения.

Тогда возможны следующие ситуации:

1) нехватка времени для получения необходимого количества информации, т.е. $\max \sum_{i=1}^{n} f_i(x_i) < F$;
2) возможная хватка времени для получения необходимого количества информации, т.е. $\max \sum_{i=1}^{n} f_i(x_i) \le F$;
3) достаточно времени для получения необходимого количества информации, т.е. $\max \sum_{i=1}^{n} f_i(x_i) = F$;
4) более чем достаточно времени для получения необходимого количества информации, т.е. $\max \sum_{i=1}^{n} f_i(x_i) \ge F$.

Из условий задачи и алгоритма решения можно заключить, что для 1-го случая, СЗИ и механизмы управления ею будут недостаточны, т.е. набор применяемых процессов неэффективен и не может решить задачу полностью.

Для негативного сценария (нехватка времени) 2-го случая все как в 1-ом случае, но для его положительного сценария (минимальное время достаточно), полное решение можно получить. Кроме неэффективности реализации и управления СЗИ, также возможен вопрос о недостаточности ресурсов или о нехватке времени из-за применения неэффективных алгоритмов. В таком случае можно искать решение по алгоритму на рис. 4.

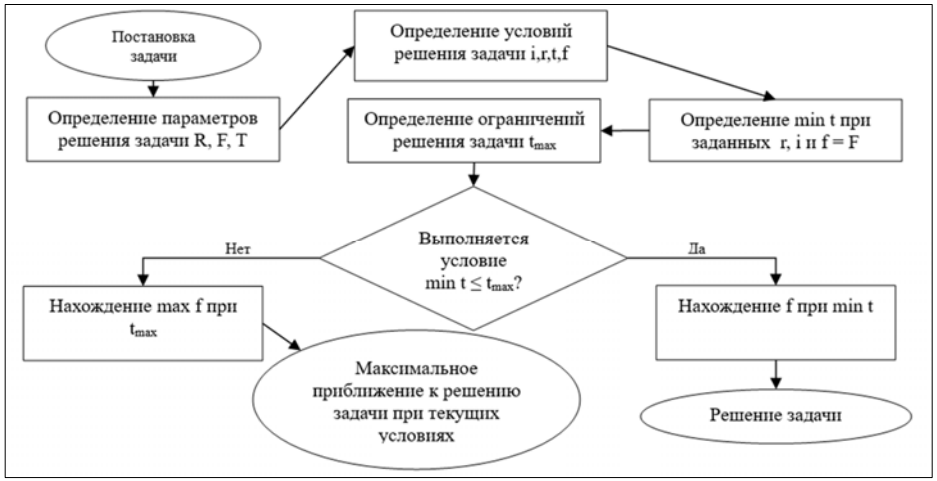

Рис. 4. Алгоритм решения задачи
Fig. 4. Algorithm for solving the problem

Как можно видеть из рис. 4, возможна ситуация нехватки времени для полного решения задачи. При этом также возможно, что нельзя оказать влияние на временные рамки, что больше затрудняет ситуацию.

Предполагается, что разрешение этой сложности возможно за счет введения в практику методику управления ИБ на базе обобщенного набора правил логического вывода ОДЭС ППР, позволяющих сильно сократить временные затраты на информационные процессы и процессы принятия должного и адекватного управленческого решения.

3.2.2 Процесс управления рисками ИБ на основе ОДЭС ППР

Общее описание процесса управления рисками

Управление рисками является одним из ключевых процессов в обеспечении ИБ. В данный момент есть множество методик управления рисками ИБ. Ключевым понятием всех методик является понятие «угроза ИБ».

Главное предназначение процесса управления рисками ИБ состоит в идентификации, анализе и контроле мер, учитывающих вероятности имплементации угроз ИБ, а по типу и составу защищаемого ИА, математически просчитать потенциальную величину потерь от этой имплементации. Эти потери зависят от стоимости актива (важности актива) и опасности имплементации угрозы. «Стоимость актива» или «Важность актива» может принимать следующие значения: «Высокая», «Средняя», «Низкая». Угроза ИБ, вместе с теми на рис. 3, описывается следующими основными параметрами: объект воздействия угрозы (актив\тип актива); источник возникновения угрозы; уязвимости, используемые в процессе имплементации угрозы; способ имплементации угрозы, посредствам использования присущей ей уязвимостей; деструктивное воздействие, возникающее в процессе имплементации угрозы; вероятность имплементации угрозы; опасность имплементации угрозы. Данные параметры взаимосвязаны (рис. 5.). С учетом параметров актива для оценки рисков ИБ получим рис. 6.

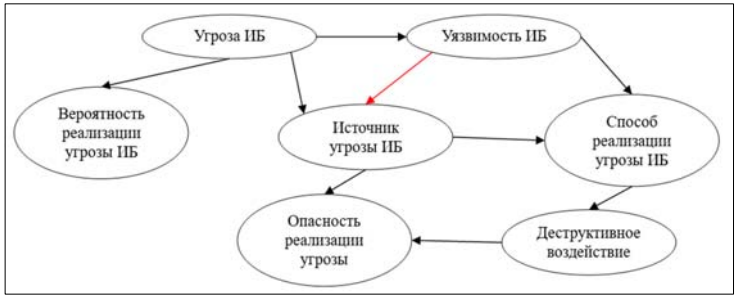

Рис. 5. Взаимосвязь параметров угроз ИБ
Fig. 5. Interrelation of IS threat parameters

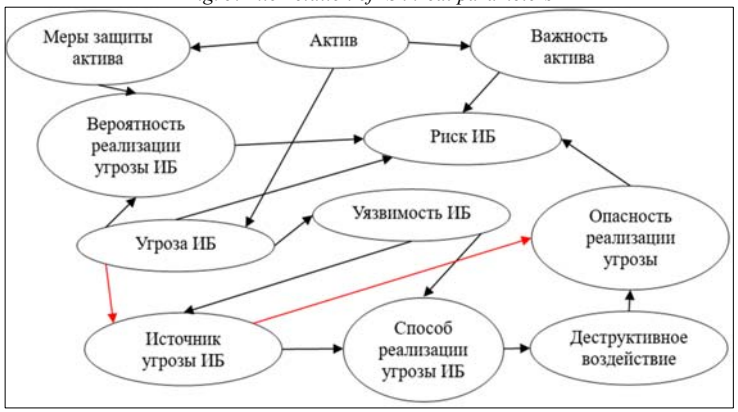

Рис. 6. Взаимосвязь параметров актива и угроз ИБ
Fig. 6. Relationship between asset parameters and IS threats

Исходя из рис. 6 видно, что для каждого актива можно получить дерево вида, представленного на рис. 7, позволяющего легко анализировать данный актив.

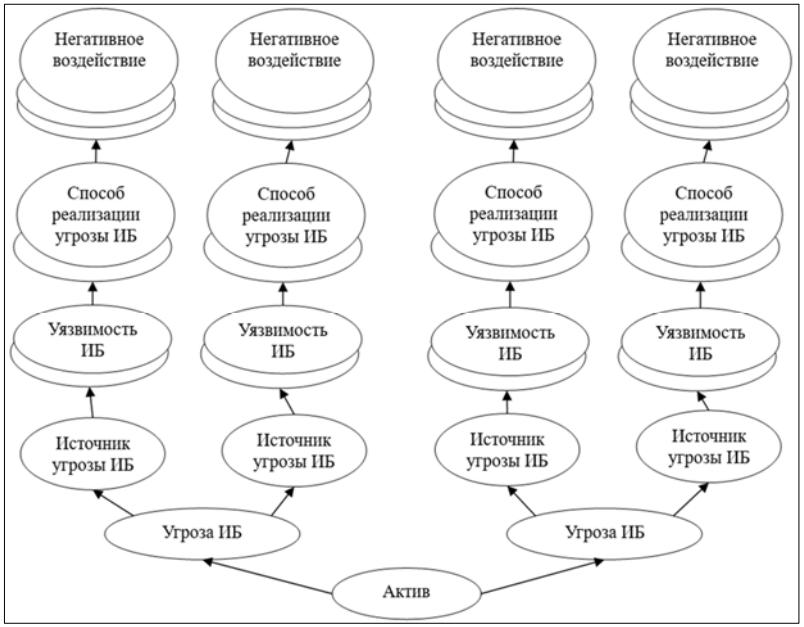

Рис. 7. Дерево угроз актива
Fig. 7. Asset threat tree

При управлении рисками ИБ важной задачей является контроль и учет контрмер (мероприятий по защите актива). По контрмерам и их параметрам можно получить вероятность имплементации угрозы, являющуюся ключевым при создании модели угроз и при расчете рисков. Расчет рисков выполняется на основе мнений всех экспертов, полученных методом экспертной оценки. Такой подход обладает следующими недостатками: субъективная оценка эксперта; разрозненность параметров, используемых экспертами; рутинность протекания процесса; длительность периода проведения оценки, вызванная необходимостью постоянной актуализации и переоценки информации, большим объемом анализируемой информации, большим количеством связанных параметров, используемых при оценке; сомнительность полученных результатов, с учетом человеческого фактора; трудоемкость процесса; отсутствие возможности дальнейшего использования и актуализации собранной информации.

Эти проблемы могут быть решены применением средств автоматизации на основе метода ОДЭС ППР. В данном методе используется онтология, полученная в результате онтологического инжиниринга (конструирования онтологической базы знаний) ПрО «Управление рисками ИБ».

Априорная вероятность реализации угроз ИБ по методу ОДЭС ППР

Для априорного определения вероятности реализации угроз (АОВРУ) ИБ, естественно применять в ОДЭС метод экспертной оценки (МЭО). МЭО позволяет учитывать специфические особенности конкретного объекта и динамику изменения мнений экспертов по ИБ. Это помогает повысить точность оценки рисков ИБ учетом всех свойств ИС. Также применяется принцип усреднения коэффициентов (ПУК) для уменьшения погрешностей МЭО. ПУК позволяет существенно снизить среднюю погрешность МЭО. Метод управления ИБ на основе ОДЭС ППР рассматривает каждую угрозу как абстрактный дискретный объект со своим набором взаимосвязанных параметров.

АОВРУ состоит в: определении проблемной области (вероятности возникновения угроз ИБ), для исключения комбинаторного взрыва; формировании группы экспертов; инженерии знаний экспертов – онтологический инжиниринг; формировании рабочей базы данных – заполнить онтологию; формализации принятия решений при получении результатов – рассуждении и логическом выводе.

С применением МЭО и ПУК нужно выполнить ещё и следующие пункты: Определение возможности осуществления способа реализации МЭО; Усреднение коэффициентов, полученных от экспертов.

Для начального наполнения онтологии знаниями, группа экспертов по ИБ предлагается для заполнения матрица из табл. 1.

Для применения АОВРУ необходимо сначала провести анализ всех угроз ИБ, найденных при просчете актуальности угроз с целью определения всех связанных с ними способов имплементации.

Табл. 1. Матрица оценки связи источника угроз и способа реализации угроз ИБ
Table 1. Matrix for assessing the connection between the source of threats and the method of implementation of IS threats

	Способ реализации	Способ реализации 1	Способ реализации 2	…	Способ реализации *M*
Источник угрозы					
Источник угрозы 1					
Источник угрозы 2					
…					
Источник угрозы *N*					

Ячейка матрицы заполняется экспертом следующим образом: невозможна (Н\В) – если, по мнению эксперта, способ реализации не используется источником угрозы; низкая (Н) – если, по мнению эксперта, способ реализации слабо используется источником угрозы; средняя (С) – если, по мнению эксперта, способ реализации нормально используется источником угрозы; высокая (В) – если, по мнению эксперта, способ реализации часто используется источником угрозы.

Данные качественные значения имеют следующие количественные оценки: Н\В = 0; Н = 0,2; С = 0,5; В = 1. Конечная матрица k_r возможности реализации угроз (ВРУ) после заполнения всеми экспертами имеет вид:

$$k_r = \sum_{i=1}^{n} \begin{bmatrix} 11 & \cdots & 1M \\ \vdots & \ddots & \vdots \\ N1 & \cdots & NM \end{bmatrix}_{k_i},$$

где i – число экспертов, N число источников угроз, а M – число способов реализации. При этом возможность реализации V_i угрозы ИБ i описывается набором всех способов реализации данной угрозы $E_i \in M$. Показатель ВРУ V_i нарушителем J рассчитывается как среднее арифметическое полной суммы показателей строки J матрицы k_r для всех E_i.

В зависимости от используемой методологии расчета актуальности угроз и рисков ИБ, коэффициенты подлежат дополнительной трактовке, однако исходя из общей логики метода разброс возможных значений итоговых показателей следует трактовать так: $V_i \in [0,\ 0{,}2)$ – нереализуема; $V_i \in [0{,}2\ ,\ 0{,}5)$ – мало вероятно реализуема; $V_i \in [0{,}5\ ,\ 0{,}8)$ – вероятно реализуема; $V_i \in [0{,}8\ ,\ 1)$ – крайне вероятно реализуема.

Степень опасности реализации угроз ИБ по методу ОДЭС ППР

Оценка степени опасности реализации угроз (СОРУ) ИБ основывается на принципах ОДЭС ППР. При этом принимаются во внимание величину и степень влияния возможных негативных последствий при реализации угрозы (ВНПРУ). В основном СОРУ формализуется в виде денежной суммы (см. ниже), однако это не применяется, если последствия реализации угроз ИБ неоценимы в денежном эквиваленте, или, если эта оценка неприемлема по степени важности самих активов. Тогда построение модели угроз имеет цель не минимизация финансовой потери, а определение наиболее уязвимых мест в СЗИ и формирование перечня контрмер.

Для оценки СОРУ ИБ будут применяться в ОДЭС МЭО и ПУК. Как и выше метод управления ИБ на основе ОДЭС ППР рассматривает каждую угрозу как абстрактный дискретный объект со своим набором взаимосвязанных параметров. При этом СОРУ будет меняться относительно важности актива.

Оценка СОРУ состоит в определении проблемной области (степень опасности угроз ИБ), для исключения комбинаторного взрыва; формировании группы экспертов; инженерии знаний экспертов – онтологический инжиниринг; формировании рабочей базы данных – заполнить онтологию; формализации принятия решений при получении результатов – рассуждении и логическом выводе.

С применением МЭО и ПУК нужно выполнить ещё и следующие пункты: определение СОРУ деструктивного воздействия на основе МЭО; усреднение коэффициентов, полученных от экспертов; определение важности защищаемых активов.

Для начального наполнения онтологии знаниями группа экспертов по ИБ предлагается для заполнения матрица из табл. 2.

Для оценки СОРУ необходимо сначала провести анализ всех угроз ИБ, найденных при просчете актуальности угроз с целью определения всех связанных с ними ВНПРУ.

Табл. 2. Матрица оценки связи источника угроз и ВНПРУ ИБ
Table 2. Matrix for assessing the connection between the source of threats and the impact of possible negative consequences in the implementation of the IS threat

	ВНПРУ	ВНПРУ 1	ВНПРУ 2	…	ВНПРУ M
Источник угрозы					
Источник угрозы 1					
Источник угрозы 2					
…					
Источник угрозы N					

Ячейка матрицы заполняется экспертом следующим образом: Низкая (Н) – если, по мнению эксперта, ВНПРУ имеет низкую степень влияния на защищаемые от источника угрозы активы; Средняя (С) – если, по мнению эксперта, ВНПРУ имеет среднюю степень влияния на защищаемые от источника угрозы активы; Высокая (В) – если, по мнению эксперта, ВНПРУ имеет высокую степень влияния на защищаемые от источника угрозы активы.

Данные качественные значения имеют следующие количественные оценки: Н = 0; С = 0,5; В=1. Конечная матрица k_r СОРУ после заполнения всеми экспертами имеет вид:

$$k_r = \sum_{i=1}^{n} \begin{bmatrix} 11 & \cdots & 1M \\ \vdots & \ddots & \vdots \\ N1 & \cdots & NM \end{bmatrix}_{k_i},$$

где i – число экспертов, N число источников угроз, а M – число ВНПРУ. При этом степень опасности D_i угрозы ИБ i описывается набором всех ВНПРУ $Q_i \in M$.

Показатель СОРУ D_i нарушителем J рассчитывается как среднее арифметическое полной суммы показателей строки J матрицы k_r для всех Q_i.

В зависимости от используемой методологии расчета актуальности угроз и рисков ИБ, коэффициенты подлежат дополнительной трактовке, однако исходя из общей логики метода разброс возможных значений итоговых показателей следует трактовать так: $D_i \in [0\ ,\ 0{,}4)$ – низкая степень опасности; $D_i \in [0{,}4\ ,\ 0{,}8)$ – средняя степень опасности; $D_i \in [0{,}8\ ,\ 1)$ – высокая степень опасности.

Формализация СОРУ в виде денежной суммы производится следующим образом:

Для каждого актива определим денежную стоимость с точки зрения его материальной (например, физической инфраструктуры) и нематериальной (например, репутации организации и цифровой информации) ценности для организации. Оценивая общую стоимость влияния для каждого актива, используем следующие категории: стоимость замены, затраты на обслуживание и поддержание работоспособности, затраты на обеспечение избыточности и доступности, репутация организации (репутация на рынке), эффективность работы организации, годовой доход, конкурентное преимущество, внутренняя эффективность эксплуатации, правовая и регулятивная ответственность.

Еще один подход к определению стоимости активов основан на сотрудничестве с группой управления финансовыми рисками, у которой должны быть страховые оценки и информация о страховом покрытии для соответствующих активов.

В результате получится перечень активов с указанием их приоритетов и приблизительной оценки их денежной стоимости для организации.

Теперь можно определить степень ущерба в процентах, который может быть причинен активу. Для этого используем уровень подверженности воздействию, определенный в ходе анализа и обсуждения собранных данных. Полученное значение называется фактором подверженности воздействию.

Следующий шаг состоит в получении количественной оценки влияния путем умножения стоимости актива C_j на фактор подверженности воздействию f_j. Тогда СОРУ D_i в деньгах определяется суммированием всех количественных оценок влияния на активы для данной угрозы, т.е.

$$D_i = \sum_{j=1}^{L} C_j * f_j$$

где D_i степень опасности угрозы ИБ i в деньгах, L - число активов, C_j – стоимость j-ого актива, f_j - фактор подверженности воздействию j-ого актива.

Постаприорная оценка возможности реализации угроз ИБ

На основе определении пост априорной оценки возможности реализации угроз (ПАОВРУ) ИБ положены структура ОДЭС ППР и МЭО. Базой для принятия решений при оценке ВРУ ИБ являются знания в статической и динамической частях онтологии. Динамическая часть онтологии содержит знания по ИС, включая сведения об ИА, средствах и механизмах ЗИ, а также свойства и метазнания по каждому ИА, по каждой СЗИ.

Статическая же часть онтологии содержит служебную информацию и правила взаимодействия, как в самой статической части, так и в динамической.

Статическая часть онтологии содержит: знания о каждой из имеющихся угроз ИБ, включая: объект воздействия (ИА), способы имплементации уязвимости, предусмотренные данной угрозы; условия существования данной угрозы для защищаемого ИА.

Правила логического вывода для ответа на вопросы (запросы) строятся на основе следующих привязок параметров друг к другу: «Тип ИА» – «Угроза»; «Угроза» – «Условие возникновения угрозы (УВУ)»; «Угроза» – «Меры защиты от угрозы (МЗОУ)»; «МЗОУ» – «Требования»; «МЗОУ» – «Ограничения»; «МЗОУ» – «Средства защиты от угрозы (СЗОУ)»;

«МЗОУ» – «Стандарты и НПД»; «Требования» – «Ограничения»; «СЗОУ» – «Стандарты и НПД» и т.д.

Поскольку УВУ прямо связано с типом ИА и его угроз, то оценка параметра «УВУ» будет меняться в значениях (α): 0 – УВУ отсутствует, 1 – УВУ существует.

УВУ определяется по общему мнению всех экспертов.

Опираясь на знаниях об УВУ и типах ИА воздействия угрозы, на этапе наполнения онтологии формализуются МЗОУ, для каждой из которых заполняются СЗОУ. Для защиты от угрозы набором МЗОУ, каждая МЗОУ будет иметь свой вес в виде процентной градации степени защиты от угрозы (X).

Для каждого СЗОУ конкретной МЗОУ определяется максимальное числовое значение, определяющее полноту перекрытия МЗОУ данным СЗОУ (R). На основе мнения экспертов по ИБ, R может принимать следующие значения: 0 – СЗОУ отсутствует; 3 – СЗОУ не обладает подтверждением реализации требуемых функций, корректности их настройки; 5 – СЗОУ обладает подтверждением требуемых функций, но отсутствуют сведения о корректности; 7 – СЗОУ обладает подтверждением требуемых функций и есть подтверждения корректности настройки.

Расчет ВРУ V производится по формуле:

$$\begin{cases} V = \alpha * \dfrac{\left(\left(R_{1_{max}} - R_{1_{par}}\right) * \dfrac{X_1}{100}\right) + \left(\left(R_{2_{max}} - R_{2_{par}}\right) * \dfrac{X_2}{100}\right) + \left(\left(R_{n_{max}} - R_{n_{par}}\right) * \dfrac{X_n}{100}\right)}{R_{max}} \\ X_1 + X_2 + \cdots + X_n = 100, \\ \alpha \in [0{,}1]. \end{cases}$$

$R_{i_{par}}$– текущее значение R полноты перекрытия СЗОУ i-ой МЗОУ.

X_i– коэффициент X степени защиты от угрозы v-ой МЗОУ.

α – наличие УВУ.

Достоинства подхода на базе ОДЭС ППР

Достоинства подхода на основе ОДЭС ППР состоят в: онтологической формализации ПрО «Управление рисками ИБ»; возможности применения современных спецификаций, технологий и средств онтологического инжиниринга, например, семантического веба и protégé, для управления рисками ИБ; исключении субъективной неопределенности экспертов по ИБ; объективности оценки ВРУ, с учетом общего мнения группы экспертов; формализации всех применяемых параметров оценки ВРУ ИБ; автоматизации и интеллектуализации выполнения процесса; учете требований и действующих средств и мер ЗИ; существенном сокращении времени проведения оценки; упрощении процессов проведения переоценки и актуализации; сокращении нагрузки на аналитиков по ИБ; установлении логической взаимосвязи параметров, применяемых при оценки ВРУ ИБ; статистической достоверности полученных результатов; минимизации человеческого фактора; возможности дальнейшего использования и актуализации собранной информации, достигаемой посредством применения средств автоматизации; Гибкость метода управления рисками ИБ, учитывающего не только положения Российской и международной нормативно-правовой документации по ИБ, но и внутренние и отраслевые требования, характерные для специфики деятельности конкретной организации; Снижение временных и материальных затрат на поддержание процессов обеспечения ИБ;

Основой предлагаемого метода является онтологический подход и принципы ДЭС ППР, а МЭО используется только для учета мнения экспертов и как один из многих путей заполнения онтологии данными наряду с автоматическими методами. Система базируется на детально разработанной онтологии ПрО «Управление рисками ИБ». Кроме МЭО существует расширение онтологической модели по принципу объединения онтологий разного уровня представления или обучения. Также существует расширение аналитических способностей

ОДЭС ППР добавлением новых правил логического вывода экспертным методом, методами DataMining и машинного обучения.

Наш онтологический подход позволит эффективно управлять знаниями для эффективного управления ИР.

Применение правил логического вывода обеспечивает получение детальной картины принятого решения и предоставляет возможность оценить степень влияния на систему взаимодействующих факторов.

3.3 Структура подхода на основе ОДЭС ППР

Структура типовой ОДЭС ППР в управлении рисками ИБ включает следующие компоненты.

- Онтологию ПрО «Управление рисками ИБ» с разработанными классификаторами от экспертной группы, поддержанной группой инженеров по знаниям. Онтология содержит все о ПрО, в том числе методики определения актуальности угроз, уязвимостей и рисков ИБ; методики оценки эффективности работы СЗИ и её составных частей; методики проведения аудита и оценки степени соответствия требованиям внешних и внутренних регулирующих органов; правила логического вывода. Она может быть создана в Protégé.
- Пользовательский интерфейс для пользователей и экспертов, который может быть создан средствами Java и Jena или на базе Protégé.
- Интеллектуальный редактор онтологии, который может быть создан средствами Java и Jena или на базе Protégé.
- Целевая аудитория пользователей системы.
- Экспертная группа, участвующая в процессе формирования требований исходных данных по самой системе и её составным частям.
- Группа инженеров по знаниям, осуществляющих онтологический инжиниринг под контролем экспертной группы.
- Рабочая память системы, обеспечивающая взаимодействие данных.
- Механизмы логического вывода, осуществляющего анализ исходных и актуализированных знаний на основе сформированных экспертами логических правил поведения системы.
- Подсистема объяснений, отвечающая за аналитическое обоснование принятых решений по результатам обработки знаний механизмами логического вывода.

3.4 Оценка эффективности СЗИ на основе ОДЭС ППР

Для оценки эффективности подхода необходимо сравнить эффективность СЗИ на его основе и СЗИ без его применения. Для этого требуется определить главные факторы, влияющие на эффективность СЗИ. Сравнение будем проводить математически, суммируя частные коэффициенты эффективности (суммируются взвешенные суммы частных факторов влияния на эффективность СЗИ), т.е. Коэффициент эффективности СЗИ рассчитывается по формуле:

$$W(S_i) = \sum_{f=1}^{N} \alpha_f s_f(S_i),$$

где: S_1 – исходный подход к управлению рисками ИБ в компании EDM SA Республики Мали;

S_2 – подход к управлению рисками ИБ на основе ОДЭС ППР;

$W(S_i)$ – коэффициент эффективности СЗИ подхода;

f – индекс фактора влияния;

N – количество факторов влияния;

αf – вес факторов $s_f(S_i)$ в общем весе эффективности СЗИ, при этом $\sum_{f=1}^{N} \alpha_f = 1,\ 0 \le \alpha_f \le 1$.

Факторы, имеющие высокое влияние на эффективность СЗИ предоставлены экспертами по ИБ малийской энергетической компании EDM SA после опроса. В результате получены следующие критерии для оценки эффективности: время на внедрение процесса управления рисками ИБ; время на сбор исходных данных от процесса управления рисками ИБ; время на обработку собранной от процесса управления рисками ИБ информации; время на актуализацию собранной от процесса управления рисками ИБ информации; время на анализ полученных результатов; время на ПУР.

Эксперты оценили каждый фактор, при этом высокий коэффициент получил тот подход СЗИ, в котором время на выполнение полного цикла по процессу управления рисками ИБ было минимальным. Оценки экспертов указаны в табл. 3. Уточняем, что данные значения были выставлены экспертами малийской энергетической компании EDM SA и авторы данной работы не отвечают за их корректность.

Табл. 3. Данные для расчета и анализа эффективности исходного подхода к ИБ и подхода к ИБ на основе ОДЭС ППР

Table 3. Data for calculating and analyzing the effectiveness of the initial approach to IS and an approach to IS based on decision support with ontological dynamic expert systems

	Факторы, влияющие на эффективность СЗИ	**Степень значимости коэффициента**	**Частный показатель исходного подхода управления ИБ**	**Частный показатель подхода ОДЭС ППР управления ИБ**
1	**Временные затраты на внедрение процесса ИБ**	0,25	1	0,1
2	**Временные затраты на сбор исходных данных от процесса ИБ**	0,10	0,5	0,9
3	**Временные затраты на обработку собранной от процесса ИБ информации**	0,15	0,3	0,8
4	**Временные затраты на актуализацию собранной от процесса ИБ информации**	0,15	0,4	1
5	**Временные затраты на принятие управленческого решения**	0,25	0,6	1
6	**Временные затраты на анализ полученных результатов**	0,10	0,3	0,8
	Итоговый коэффициент эффективности		**0,58**	**0,95**

Расчет коэффициента эффективности СЗИ с использованием исходного подхода управления ИБ $S1$:

$$W(S_1) = 0{,}25 * s_1(S_1) + 0{,}1 * s_2(S_1) + 0{,}15 * s_3(S_1) + 0{,}15 * s_4(S_1) + 0{,}25 * s_5(S_1) + 0{,}1 * s_6(S_1) \quad \leftrightarrow$$
$$W(S_1) = 0{,}25 * 1 + 0{,}1 * 0{,}5 + 0{,}15 * 0{,}3 + 0{,}15 * 0{,}4 + 0{,}25 * 0{,}6 + 0{,}1 * 0{,}3 \quad \leftrightarrow$$
$$W(S_1) = 0{,}58$$

Расчет коэффициента эффективности СЗИ с использованием подхода управления ИБ на основе ОДЭС ППР $S2$:

$$W(S_2) = 0{,}25 * s_1(S_2) + 0{,}1 * s_2(S_2) + 0{,}15 * s_3(S_2) + 0{,}15 * s_4(S_2) + 0{,}25 * s_5(S_2) + 0{,}1 * s_6(S_2) \quad \leftrightarrow$$
$$W(S_2) = 0{,}25 * 1 + 0{,}1 * 0{,}9 + 0{,}15 * 0{,}8 + 0{,}15 * 1 + 0{,}25 * 1 + 0{,}1 * 0{,}8 \quad \leftrightarrow$$
$$W(S_2) = 0{,}94$$

Из расчетов видно преимущество подхода управления ИБ на основе ОДЭС ППР. Этот подход сильно снижает временные затраты и увеличивает эффективность СЗИ на 36%.

4. Сравнительный анализ существующих подходов и методик к управлению рисками ИБ и ОДЭС ППР

Сравнение проводится на основе указания преимуществ и недостатков каждого подхода. В табл. 4 указаны описание, сильные и слабые стороны некоторых современных подходов к управления рисками ИБ, в том числе ОДЭС ППР.

Табл. 4. Анализ некоторых современных подходов к управлению рисками ИБ
Table 4. Analysis of some modern approaches to information security risk management

Подход/ Методика	**Описание**	**Сильные стороны**	**Слабые стороны**
Метод Дельфи [31], [32]	Формальный метод чисто экспертного прогнозирования; основывается только на экспертных оценках.	Позволяет оценить специфику каждой конкретной ситуации, способствует выработке независимого мышления членов экспертной группы и позволяет получить взвешенную оценку рассматриваемого вопроса.	Сложность в выборе большой группы компетентных экспертов, чрезмерную субъективность оценок.
Статистические методы (RiskMetrics Value-at-Risk VaR, Имитационное моделирование и т.п.) [30],[31]	Заключаются в определении вероятности возникновения потерь на основе статистических данных предшествующего периода и установлении области (зоны) риска, коэффициента риска и других параметров риска.	Позволяет проводить анализ и оценку различных вариантов развития событий и учитывать разные факторы рисков в рамках одного подхода с учетом накопленных статистических данных	Необходимость использования в данных методах вероятностных характеристик.
Методика RiskWatch [30]. США.	Обнаружение уязвимостей на основе анкетирования с использованием более чем 600 вопросов, разделенных на классы. В качестве показателей для оценки и управления рисками используются	Позволяет обнаруживать угрозы и уязвимости, оценивать уровни выделенных факторов,	Не учитывает организационные и административные уровни, не реализует все аспекты комплексной защиты информации,

	прогнозируемые среднегодовые потери (Annualized Loss of Expectancy, ALE) и оценка возврата от инвестиций (Return on Investment, ROI). Ожидаемая частота реализации угроз определяется в терминах среднегодовой оценочной частоты угрозы (Annual Frequency Estimate, AFE). База знаний RiskWatch определяет для каждой угрозы стандартную оценочную частоту (Standard Annual Frequency Estimate, SAFE).	оценивать соблюдение требований стандартов, прогнозировать величину ущерба и вырабатывать контрмеры с максимальным возвратом вложений. Содержит большую базу знаний, содержащую информацию по активам, угрозам, уязвимостям, видам ущерба, мерам защиты, а также опросные листы для оценки факторов риска. Для вычисления величины риска используется локальная оценочная частота угрозы (Local Annual Frequency Estimate, LAFE), определяемая пользователем самостоятельно на основании значения SAFE.	математическое ожидание ущерба не отражает с системных позиций концепты риска.
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [31]	Разработана в университете Карнеги-Мелон в 2007 году, описывает подход к качественной оценке рисков. Осуществляет оперативную оценку критических угроз, активов и уязвимостей.	Предусматривает регулярное проведение оценки рисков и обновление их величин как части процесса оценки рисков, простота и прозрачность, итеративный подход к анализу, невысокие трудозатраты.	Не дает количественной оценки рисков, отсутствие подробных баз знаний, отсутствие возможности оценки рисков в деньгах.
COBIT for Risk [32],[34]	Разработана ассоциацией ISACA (Information Systems Audit and Control Association) в 2013 году и базируется на лучших практиках управления	Доступ к общей библиотеке COBIT, апробированный метод, признается международными	Высокая сложность и трудоемкость сбора исходных данных, ресурсоемкость, отсутствие

	рисками (COSO ERM, ISO 31000, ISO\IEC 27xxx и др.).	институтами, наличие каталогов рисковых сценариев и «ИТ-контролей», может быть использован при аудите.	возможности оценки рисков в деньгах.
FRAP (Facilitated Risk Analysis Process) [32],[34]	Разработана компанией Peltier and Associates в 2000 году, описывает подход к качественной оценке рисков. Целью методики является выявление, оценка и документирование состава рисков информационной безопасности для заранее определенной области исследования. В качестве области исследования может быть выбрана информационная система, приложение, бизнес-процесс или другая часть инфраструктуры организации, нуждающаяся в оценке рисков информационной безопасности.	Простота и прозрачность, минимальные трудозатраты, минимальное количество участников проектной команды.	Отсутствие жестко регламентированного процесса управления рисками ИБ и детальных баз знаний, отсутствие возможности глубокой декомпозиции, подробной и точной оценки рисков, отсутствие возможности оценки рисков в деньгах.
Метод CRAMM (CCTA Risk Analysis and Management Method). [31],[32] Великобритания	Применяется как государственный стандарт, обладает большой библиотекой мер защиты, состоящей примерно из 3500 наименований, разделенной на 70 логических групп. Выбор мер защиты также может определяться в соответствии с требованиями стандартов BS7799:2005/ISO 27001.	Комплексный подход к оценке рисков, применение технологии оценки угроз и уязвимостей по косвенным факторам с возможностью верификации результатов, хорошо апробирован, хорошая система моделирования информационных технологий, большая БД для оценки рисков и выбора контрмер, использование в качестве средства аудита, универсальность и адаптируемость под профили	Необходимость высокой квалификации аудитора, плохая адаптивность к новым информационным системам, относительно трудоемкий, сложная отчетность, трудности при адаптации к потребностям конкретной компании в связи с недоступностью пользователям в ПО CRAMM модификации базы знаний и шаблонов отчетов, ПО CRAMM имеется только на английском языке, дорогая лицензия от 2000 до 5000 долларов.

		разных организаций.	
MSAT «Microsoft Security Assessment Tools» [33]	Предложена корпорацией Microsoft в 2006 году. Оценка риска состоит из определения профиля риска для бизнеса и оценки индекса эшелонированной защиты, которые сравниваются для измерения распределения риска во всех областях анализа.	Прозрачность, комбинирование качественного и количественного подходов, охват всех аспектов управления рисками, возможность оценки рисков ИБ в деньгах, наличие базы знаний.	Отсутствие типовых рисковых сценариев, высокая трудоемкость процесса управления рисками, плохо учитывает особенностей компаний на территории РФ, не работает по требованиям российского законодательства и стандартов, не измеряет эффективность применяемых защитных мер.
PTA (Practical Threat Analysis) [32]	Количественная оценка рисков. На входе поступают сведения об активах, угрозах, уязвимостях и контрмерах. На выходе получаем общую стоимость активов, стоимость контрмер, уровень рисков, перечень из 5 наиболее опасных угроз.	Можно использовать как средство непрерывного управления рисками. Можно отслеживать динамику состояния защищенности объекта изменяя входные данные (данные активов, угроз, уязвимостей и контрмер), а также на основе результатов оценки рисков, можно повысить эффективность средств защиты.	Результаты оценки рисков в процентах плохо интерпретируются. Также не всегда возможна оценка актива или ущерба, наносимого угрозой, в денежных единицах как это требуется.
CORAS [32],[34]	Суть состоит в адаптации, уточнении и комбинировании таких методов проведения анализа рисков, как Event-Tree-Analysis, цепи Маркова, HazOp и FMECA. Используется технология UML, базируется на австралийском/новозеландском стандарте AS/NZS 4360: 1999 Risk Management и ISO/IEC 17799-1: 2000 Code of Practice for	Очень простой подход, потребляет мало ресурсов, проводит классификацию рисков для оценки, снижения или устранения, ликвидация угроз.	Не предусмотрена периодичность проведения оценки рисков и обновление их величин, не позволяет оценить эффективность инвестиций для внедрения мер безопасности, не дает возможности найти

	Information Security Management. В этом стандарте учтены рекомендации, изложенные в документах ISO/IEC TR 13335-1: 2001 Guidelines for the Management of IT Security и IEC 61508: 2000 Functional Safety of Electrical/Electronic/Programmable SafetyRelated.		необходимый баланс между мерами, направленными на предотвращение, выявление, исправление или восстановление информационных активов.
AURUM (Automated Risk and Utility Management) [34]	Позволяет автоматизировать управление рисками ИБ, включая объективные меры по снижению рисков с учетом всей обстановки организации. Он основан на онтологии предметной области ИБ, чтобы гарантировать, что знания об ИБ предоставляются менеджеру рисков последовательным и всеобъемлющим образом.	Онтологический подход к анализу рисков.	Информация, представленная в онтологии, включает в себя только понятия угрозы, уязвимости и контроля, что очень ограниченно по сравнению с онтологическим подходом, предложенным в данной работе.
ОДЭС ППР. Россия	Описываемая в этой статье система	См. 2.1 и 2.2.2. (Достоинства подхода на базе ОДЭС ППР). И также ОДЭС ППР учитывает все преимущества и недостатки конкурентов.	Очень большая и детальная онтология, что может в дальнейшем усложнить запросы и логический вывод, при ненадлежащем контроле и не автоматическом управлении ею методами DataMining и машинного обучения.

Преимущества ОДЭС ППР над конкурентами говорят сами за себя.

5. Заключение

В работе: приведены основные концепты ПрО «Управление рисками ИБ»; разработана онтологическая модель ПрО; приведены основные свойства концептов онтологии ПрО; указаны примерные вопросы к онтологии для извлечения знаний; разработана онтологическая модель процесса управления рисками ИБ; указаны место и роль управления рисками ИБ на основе ОДЭС ППР; описана трудность принятия управленческих решений при управлении ИБ; описан процесс управления рисками ИБ на основе ОДЭС ППР и указаны его преимущества; дано описание структуры СЗИ на основе ОДЭС ППР; выполнена оценка эффективности СЗИ на основе ОДЭС ППР. проведен сравнительный анализ существующих подходов и методик к управлению рисками ИБ и ОДЭС ППР.

На основе разработанной онтологии и подхода могут быть созданы высокоинтеллектуальные системы управления рисками ИБ и системой защиты информации в целом. Подобная система сейчас разрабатывается и будет полностью реализована и протестирована.

Список литературы / References

[1] ГОСТ Р ИСО/МЭК 27000-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология / ISO/IEC 27000-2021. Information technology. Security techniques. Information security management systems. Overview and vocabulary.

[2] ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. / ISO/IEC 27001:2005. Information technology. Security techniques. Information security management. Requirements.

[3] ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. / ISO/IEC 27000-2013. Information technology. Security techniques. Code of practice for information security controls.

[4] ГОСТ Р ИСО/МЭК 27003-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. / ISO/IEC 27003:2017. Information technology. Security techniques. Information security management systems. Guidance for implementation.

[5] ГОСТ Р ИСО/МЭК 27004-2021. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. / ISO/IEC 27004:2016. Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation.

[6] ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. / ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management.

[7] ГОСТ Р ИСО/МЭК 27006-2020. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. / ISO/IEC 27006:2015. Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems.

[8] ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения информационной безопасности. Руководство по аудиту системы менеджмента информационной безопасности. / ISO/IEC 27007:2011. Information technology. Security techniques. Guidelines for information security management systems auditing

[9] ГОСТ Р ИСО/МЭК 11799-2005. Информационная технология. Практические правила управления информационной безопасностью. / ISO/IEC 11799-2000. Information technology. Code of practice for information security management.

[10] ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. / ISO/IEC 13335-1-2004. Information technology. Security techniques. Part 1. Concepts and models for information and communications technology security management.

[11] Управление рисками в соответствии с международным стандартом ISO 31000 / Risk management in accordance with the international standard ISO 31000. Available at http://diag.by/iso-31000, accessed 27.05.2020 (in Russian).

[12] ISO 31000. Available at https://en.wikipedia.org/wiki/ISO_31000, accessed 27.05.2020.

[13] Сидоренко А.И. Новый ISO 31000:2018. / Sidorenko A.I. New ISO 31000: 2018. Available at https://riskacademyrus.wordpress.com/2018/03/10/%D0%BD%D0%BE%D0%B2%D1%8B%D0%B9-iso-310002018/, accessed 27.05.2020 (in Russian).

[14] Федеральный закон от 27.07.06 г. № 149 – ФЗ «Об информации, информационных технологиях и защите информации» / Federal Law of 27.07.06, № 149 – FZ «On Information, Information Technologies and Information Protection» (in Russian).

[15] Закон Российской Федерации «О государственной тайне» от 21.07.93 № 5485-1 (с изменениями и дополнениями) / Law of the Russian Federation "On state secrets" dated 21.07.93 № 5485-1 (with amendments and additions) (in Russian).

[16] «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» от 15 сентября 1993 г. № 912-51 / «Regulations on the state system of information protection in the Russian Federation from foreign technical intelligence services and from its leakage through technical channels» dated September 15, 1993 № 912-51 (in Russian).
[17] Федеральный закон от 27.07.06 г. № 152-ФЗ «О персональных данных» / Federal Law of 27.07.06, № 152-FZ «On Personal Data» (in Russian).
[18] Указ Президента Российской Федерации от 06.03.97 № 188 «Об утверждении Перечня сведений конфиденциального характера» / Decree of the President of the Russian Federation dated 06.03.97 № 188 «On approval of the List of confidential information» (in Russian).
[19] Федеральный закон от 28.08.2004 г. № 98-ФЗ «О коммерческой тайне» / Federal Law of 28.08.2004, № 98-FZ «On Commercial Secrets» (in Russian).
[20] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» / Decree of the Government of the Russian Federation of 01.11.2012 № 1119 «On approval of requirements for the protection of personal data during their processing in personal data information systems» (in Russian).
[21] Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 г. «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» / Decree of the Government of the Russian Federation of March 21, 2012 № 211 «On approval of the list of measures aimed at ensuring the fulfillment of obligations stipulated by the Federal Law «On Personal Data» and regulatory legal acts adopted in accordance with it, operators who are state or municipal authorities» (in Russian).
[22] Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» / Order of the FSTEC of Russia dated February 11, 2013 № 17 «On approval of requirements for the protection of information that does not constitute a state secret contained in state information systems» (in Russian).
[23] Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» / Order of the FSTEC of Russia dated February 18, 2013 № 21 «On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems» (in Russian).
[24] Конституция Российской Федерации / Constitution of the Russian Federation (in Russian).
[25] Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная указом Президента Российской Федерации от 12.09.2012 г. № 537 / The National Security Strategy of the Russian Federation until 2020, approved by the decree of the President of the Russian Federation of 12.09.2012 № 537 (in Russian).
[26] Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 / The Doctrine of Information Security of the Russian Federation, approved by the Decree of the President of the Russian Federation of December 5, 2016 № 646 (in Russian).
[27] ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения / GOST 34.003-90 Information technology. Set of standards for automated systems. Automated systems. Terms and Definitions (in Russian).
[28] ГОСТ 34.601-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания / GOST 34.601-90 Information technology. Set of standards for automated systems. Automated systems. Stages of development (in Russian).
[29] ГОСТ Р 51624-2000 Автоматизированные информационные системы в защищенном исполнении / GOST R 51624-2000 Automated information systems in a secure design (in Russian).
[30] RiskWatch International. Available at http://www.riskwatch.com, accessed 08.11.2020.

[31] Разумников С.В. Анализ возможности применения методов OCTAVE, RISKWATCH, CRAMM для оценки рисков ИТ для облачных сервисов. Современные проблемы науки и образования, no. 1, 2014 г. / Razumnikov S.V. Analysis application methods OCTAVE, RISKWATCH, CRAMM for risk assessment for it cloud services. Modern problems of science and education, ною 1, 2014 (in Russian).
[32] Куканова Н. Современные методы и средства анализа и управления рисками информационных систем компаний / Kukanova N. Modern methods and tools for analysis and risk management of information systems of companies. Available at http://citforum.ru/products/dsec/cramm/, accessed 08.11.2020 (in Russian).
[33] Средство оценки безопасности Microsoft Security Assessment Tool / Microsoft Security Assessment Tool. Available at https://technet.microsoft.com/ru-ru/security/cc185712.aspx, accessed 08.11.2020.
[34] Ekelhart A., Fenz S., Neubauer T. AURUM: A Framework for Information Security Risk Management. In Proc. of the 42nd Hawaii International Conference on System Sciences, 2009, pp. 1-10.

Информация об авторах / Information about authors

Ибрагим БУБАКАР – магистрант. Темы научных интересов: онтологическое обеспечение информационной безопасности, управление информационной безопасностью, криптографические методы защиты информации.

Ibrahim BOUBACAR – Master's Student. Research interests: ontological support of information security, information security management, cryptographic methods of information security.

Марина Борисовна БУДЬКО – кандидат технических наук, доцент, старший научный сотрудник. Научные интересы: моделирование и анализ процессов информационного взаимодействия вычислительных систем.

Marina Borisovna BUDKO – PhD, associate professor, senior researcher. Research interests: modeling and analysis of information interaction processes of computer systems.

Михаил Юрьевич БУДЬКО – кандидат технических наук, доцент. Научные интересы: информационная и функциональная безопасность телекоммуникационных сетей.

Mikhail Yurievich BUDKO – PhD, associate professor. Research interests: information and functional security of telecommunication networks.

Алексей Валерьевич ГИРИК – кандидат технических наук, доцент. Научные интересы: системное и функциональное программирование средств обеспечения информационной безопасности.

Alexei Valerievich GUIRIK – PhD, associate professor. Research interests: system and functional programming of information security tools.