Инженерный вестник Дона, №7 (2023)
ivdon.ru/ru/magazine/archive/n7y2023/8532

Построение онтологической модели для предметной области «Информационная безопасность»

Д.С. Колесникова, Е.А. Верещагина, В.Е. Гуляев

Дальневосточный федеральный университет

Аннотация: В данной статье рассмотрены аспекты проектирования онтологии для сферы информационной безопасности. Приведены примеры использования онтологий в рассматриваемой предметной области, в том числе, в области управления рисками информационной безопасности, классификации угроз и уязвимостей, мониторинга инцидентов, а также рассмотрены примеры существующих разработок онтологий по защите информации. Определена актуальность разработки правовых онтологий и значимость проектирования юридической онтологии для рассматриваемой предметной области информационной безопасности ввиду наличия большой нормативно-правой базы.
Ключевые слова: безопасность, защита информации, информационная безопасность, информация, модель предметной области, нормативный правовой акт, онтология, онтологический подход, проектирование, юридическая онтология.

На сегодняшний день информационная безопасность является одной из активно развивающихся сфер знаний. Это связано с тем, что стремительно увеличивается количество информационных ресурсов, и, соответственно, появляется потребность в их защите, когда такие данные относят к категории конфиденциальных. Кроме того, увеличивается количество угроз информационной безопасности, обнаруживается всё больше уязвимостей в системном, прикладном программном обеспечении и даже в средствах защиты информации.

Предметные области, содержащие большой объем информации (знаний), как в случае с информационной безопасностью, нуждаются в систематизации, упорядочивании данных. Для этой цели служат различные модели представления знаний (фреймовые, семантические сети, продукционная и т.д.), среди которых можно выделить онтологические [1].

Под «онтологией» понимают формальную спецификацию разделяемой концептуальной модели [2]. Онтологии позволяют формализовать знания о предметной области с использованием аппарата алгебры логики путем

определения понятий (концептов) и связей между ними. Онтологический подход применяют при проектировании систем различного назначения (обучающие, системы управления, интеллектуальные и т.д.) в различных областях знаний [3, 4]: химия, биология, юриспруденция и др.

Онтологии, в том числе, могут применяться в информационной безопасности. Некоторые из возможных применений включают:

1. Описание угроз и уязвимостей: создание онтологических моделей угроз и уязвимостей, а также связанных с ними атак, позволяет стандартизировать и классифицировать их для последующей автоматизированной обработки и анализа. Такие онтологические модели описывают типы уязвимостей, способы реализации и подход к их устранению, что в свою очередь может облегчить автоматическое обнаружение и нейтрализацию уязвимостей в информационных системах.
2. Анализ рисков: на основе онтологий можно разрабатывать методы анализа и оценки рисков в информационной безопасности.
3. Мониторинг произошедших инцидентов безопасности путем создания их формализованных описаний для последующего мониторинга и анализа.
4. Обнаружение аномальных действий: онтологии могут использоваться для формализации «здорового состояния» информационных систем, что позволит выделять отклонения и возможные инциденты.

Существуют различные примеры использования онтологий в сфере кибербезопасности. Так, в [5] авторы предложили использовать разработанную онтологию предметной области в интеллектуальной системе управления рисками информационной безопасности.

В [6] авторы привели пример построения онтологии в области защиты информации, где в качестве классов использованы наименования нормативных правовых актов (далее НПА), разделенные на подклассы в

соответствии с содержанием (структурой) НПА. Деление на подклассы в данной онтологии происходит до тех пор, пока не будут раскрыты отдельные понятия предметной области (например, «закладочное устройство», «объект информатизации» и т.д.).

В [7] группа авторов представила результаты разработки общедоступной онтологии информационной безопасности, включающей активы (объекты защиты), угрозы, уязвимости, контрмеры, а также взаимосвязи между указанными элементами. Предложено применять такую онтологию в качестве словаря по данной предметной области для общения между экспертами на одном языке, а также использовать её для формирования ответов на вопросы (например, какие меры защиты можно применить для противодействия атаке переполнения буфера и т.п.).

В данной работе предлагается к рассмотрению онтология предметной области «Информационная безопасность» с учетом актуальных положений отечественных НПА в данной области. В силу того, что НПА принимаются различными ведомствами, в разные временные промежутки, для различного рода информации и типов систем, не всегда прослеживается согласованность документов между собой. И, несмотря на то, что регуляторы стремятся совершенствовать тексты НПА, всё же происходят ситуации, когда при выпуске очередного документа обнаруживаются несогласованности, противоречия с ранее изданными НПА. Стоит отметить, что данная проблема актуальна не только для сферы информационной безопасности, но также и для других: например, правила дорожного движения, уголовное право, государственные закупки, налоговое право и т.д. Решением этой проблемы может стать создание специальных юридических (правовых) онтологий [8], призванных устранить несогласованности, систематизировать данные области знаний, и которые можно использовать в качестве словаря для

индексации юридических источников, расширения терминов, используемых в поисковых запросах и т.д.

Рассматриваемая в рамках данной работы предметная область информационной безопасности сопровождается большим количеством НПА различных типов: стандарты, законы, указы, постановления, приказы, методические документы (на рис.1 приведен фрагмент разработанной схемы связей основных НПА по информационной безопасности).

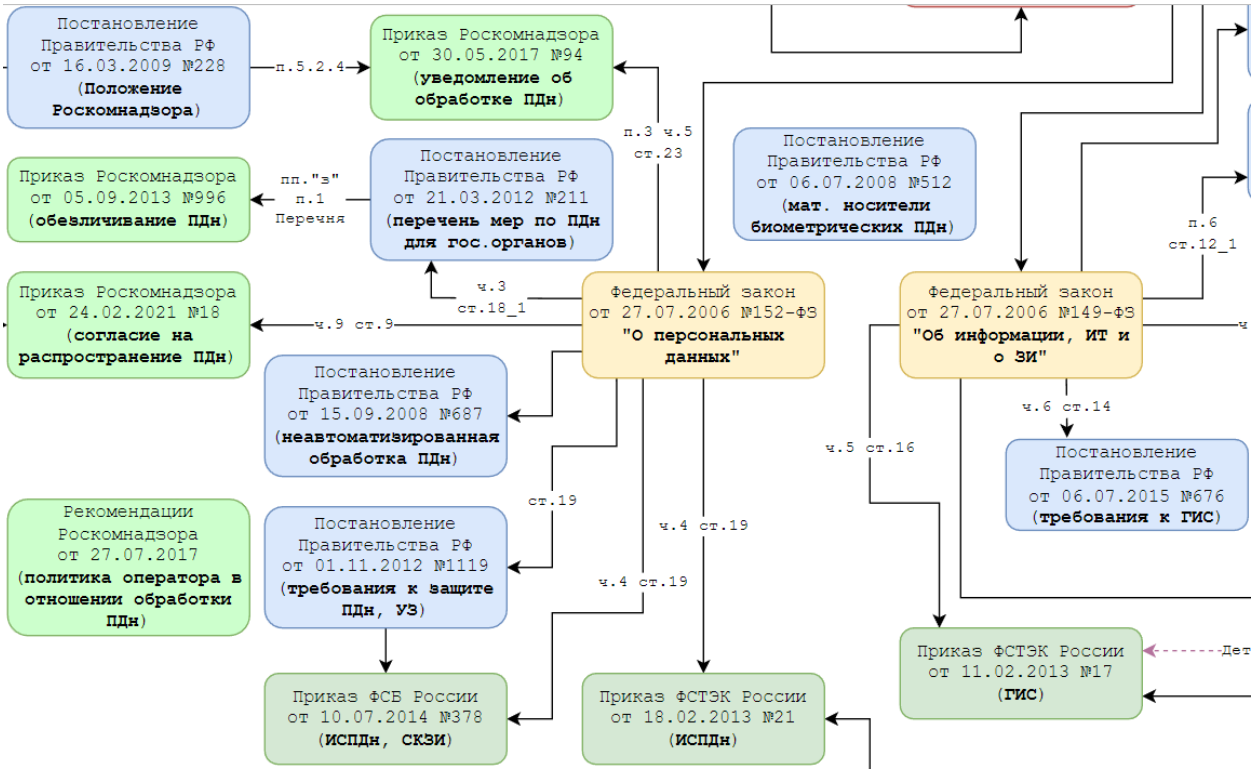

Рис. 1. – Фрагмент схемы взаимосвязей нормативных правовых актов по информационной безопасности

Важно отметить тот факт, что количество таких НПА гораздо больше, чем приведено на схеме, а также здесь не отображены некоторые типы НПА (в частности, стандарты, которых в данной области насчитывается не меньше 150 штук). Кроме того, некоторые узкие области знаний из этой сферы (например, биометрия, средства защиты информации, угрозы информационной безопасности) заслуживают создания отдельной схемы, так как количество НПА будет соразмерно (и даже больше) представленному на

рис.1. Одновременно с этим приведённая схема показывает, какой большой объём информации (и это только нормативная составляющая), требующей систематизации, имеется в данной сфере.

Предлагаемый подход к проектированию онтологии в данной области (с учетом нормативной составляющей) состоит из следующих шагов:

1. Определить перечень НПА по информационной безопасности (они должны быть актуальными, относится к рассматриваемой предметной области информационной безопасности).
2. Построить обобщённую модель онтологии предметной области с отображением взаимосвязей НПА между собой (по аналогии с представленной на рис.1 схемой).
3. Определить концепты и связи между ними для каждого НПА из перечня, определенного на этапе 1.
4. Спроектировать онтологию для каждого НПА из перечня.
5. Установить взаимосвязи между концептами различных НПА.
6. Установить взаимосвязи между разработанными на этапе 4 онтологиями.

При этом важно понимать, что потребуется постоянная актуализация такой онтологии ввиду того, что НПА могут отменяться, корректироваться, вводиться впервые.

В качестве примера на рис.2 и рис.3 изображены фрагменты разрабатываемой онтологии предметной области «Информационная безопасность», а именно – фрагменты модели онтологии для одного из важнейших НПА в сфере защиты персональных данных – Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

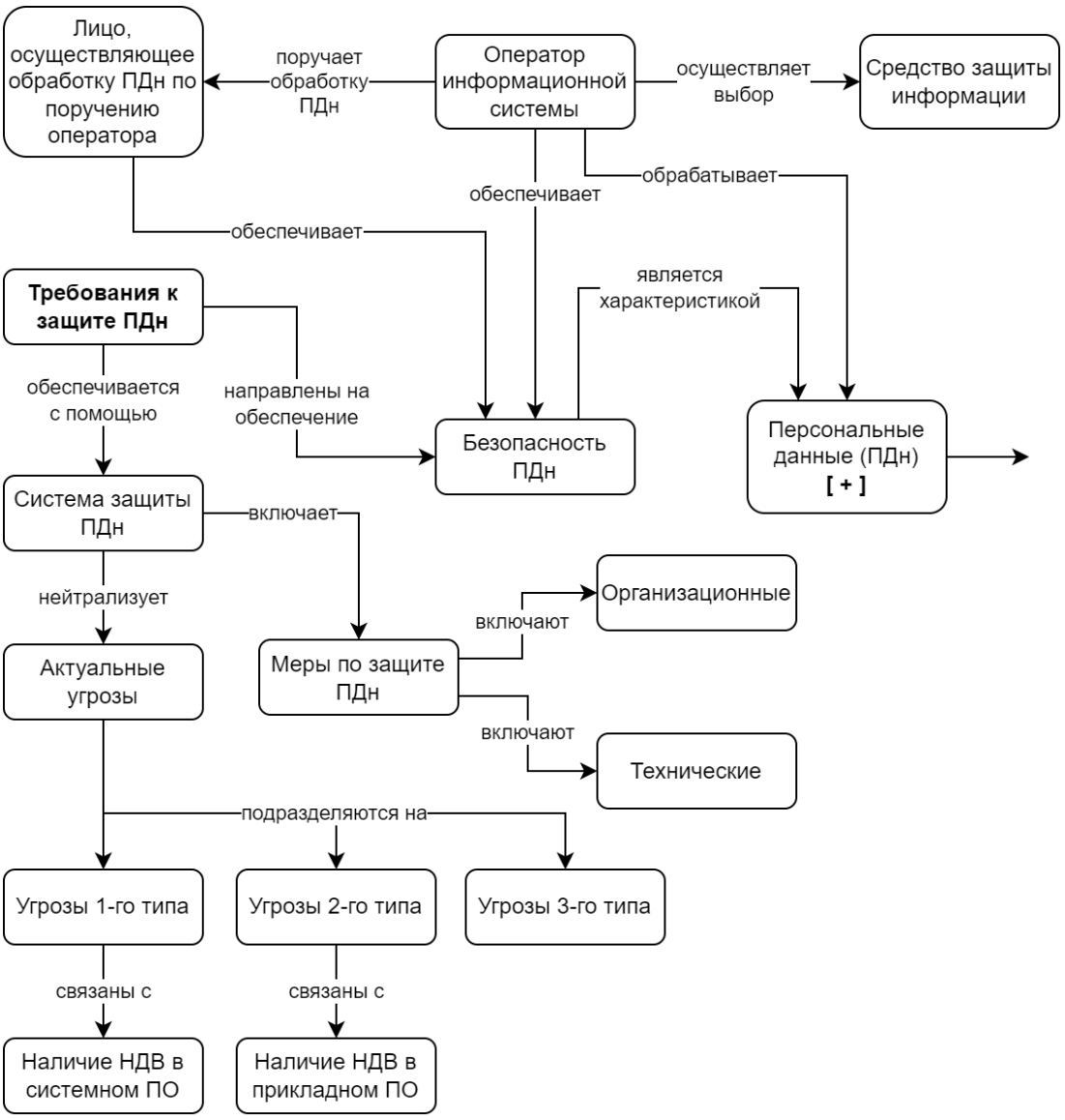

Рис. 2. – Фрагмент модели онтологии для НПА по информационной безопасности

На данной модели представлены концепты и связи между ними. По онтологии, спроектированной на основе данной модели и внедрённой в состав интеллектуальной системы, можно получать ответы на вопросы по типу: «На какие категории подразделяются персональные данные?», «На что направлены требования по защите персональных данных?», «Сколько существует уровней защищенности персональных данных?» и другие.

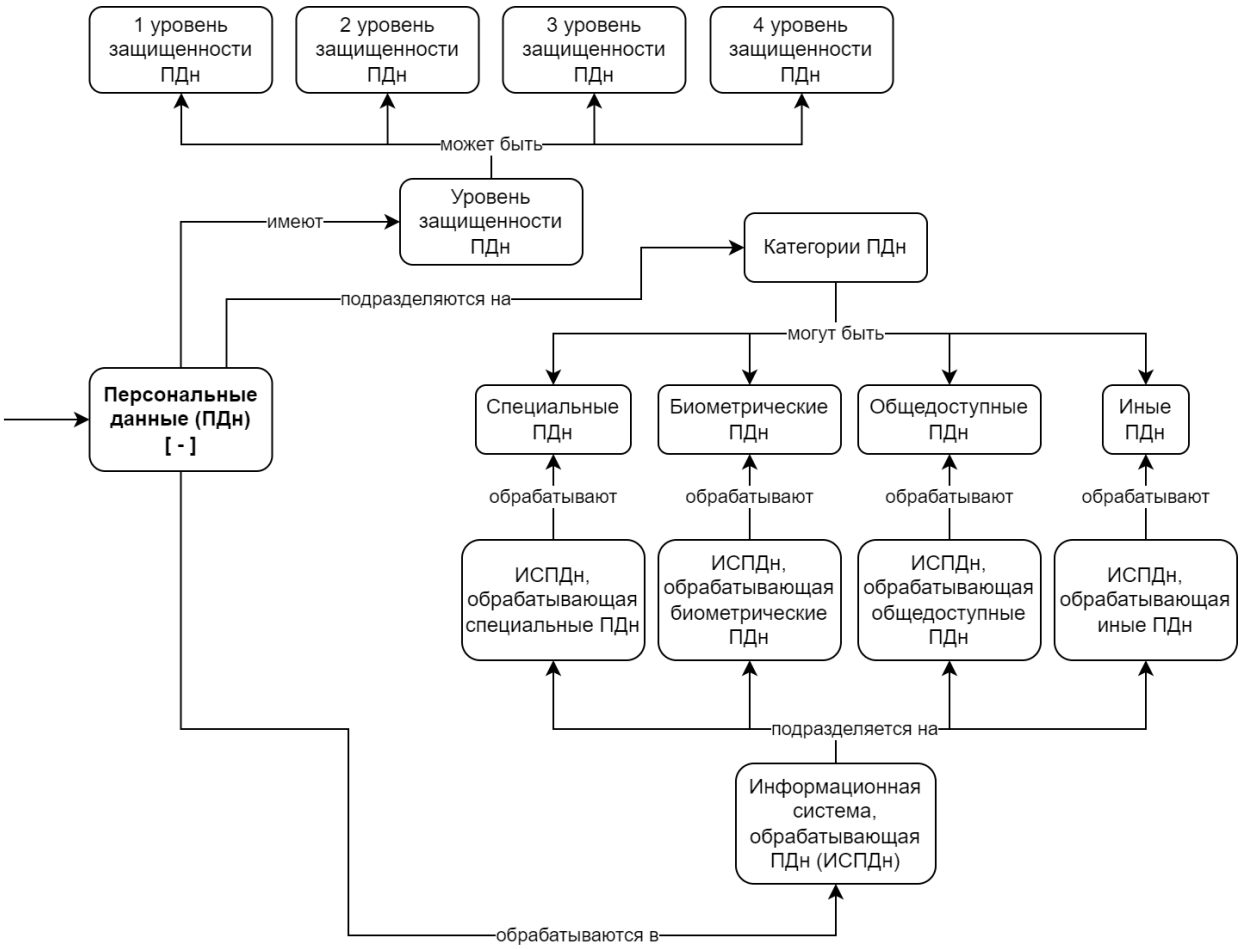

Рис. 3. – Фрагмент модели онтологии для НПА по информационной безопасности

Важным аспектом при создании любой онтологии является её применимость. Так, если говорить о рассматриваемой в рамках данной работы онтологии информационной безопасности, её можно использовать в качестве расширенного словаря специалистам и экспертам по защите информации (в том числе это может пригодиться для получения ответа на заданный вопрос, как было сказано ранее). Кроме того, такая онтология может послужить в качестве базы знаний для обучающей системы в данной области. В [9] приведен обзор существующих обучающих систем по информационной безопасности, из которого можно сделать вывод, что таких специализированных систем довольно мало, к тому же, практически у всех отсутствует взаимосвязь с нормативно-правовым полем (хотя эксперты по

защите информации призывают ориентироваться не только на НПА, но также на практические аспекты информационной безопасности, всё же знание требований законодательства является необходимым для специалистов в данной области).

На текущий момент ведется разработка моделей онтологий для других НПА в этой области (в частности, уже проанализированы НПА в области биометрии и смоделированы соответствующие онтологии), определяются концепты и связи между ними, чтобы осуществить разработку непосредственно самих онтологий на их основе. Результаты разработки в дальнейшем планируется использовать в качестве базы знаний обучающей системы по информационной безопасности. В качестве инструментальной среды используется программа Protégé.

Таким образом, проектирование и дальнейшая разработка онтологии предметной области «Информационная безопасность» (с учетом правовых аспектов) может способствовать систематизации, унификации знаний в данной области. Кроме того, такая онтология может стать словарем (справочником) для специалистов по защите информации, служить обширной базой знаний для обучающих систем, а также, с одновременным использованием технологий искусственного интеллекта [10] – быть основой для экспертной системы, способной решать различные задачи (в том числе, поиска решения) по информационной безопасности.

Литература

1. Москаленко Ю.С. Организация систем, основанных на знаниях. Владивосток: Издательский дом Дальневост. федерал. ун-та, 2013. 244 с.

2. Гаврилова Т.А., Кудрявцев Д.В., Муромцев Д.И. Инженерия знаний. Модели и методы. 6-е изд. СПб.: Лань, 2023. 324 с.

3. Feilmayr C., Wöß W. An analysis of ontologies and their success factors for application to business // Data & Knowledge Engineering. 2016. №101. С. 1-23.

4. Гарин М.С., Романенко Е.В. Интеллектуальный семантически ориентированный подход к автоматизации работы туристического агентства // Инженерный вестник Дона, 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/811.

5. Бубакар И., Будько М.Б., Будько М.Ю., Гирик А.В. Онтологическое обеспечение управления рисками информационной безопасности // Труды ИСП РАН. 2021, том 33. №5. С. 41-64.

6. Попов М.А., Федоров Д.Ю. Пример построения онтологии в области защиты информации // Защита информации в компьютерных системах. 2017. С. 13-19.

7. Herzog A., Shahmehri N. An Ontology of Information Security // International Journal of Information Security and Privacy. 2007. №1 (4). С. 1-23.

8. Миролюбова С.Ю. Правовые онтологии в машиночитаемом формате - инструмент продвижения юридических знаний в семантической сети // Мониторинг правоприменения. 2022. №1 (42). С. 39-45.

9. Колесникова Д.С., Рудниченко А.К. Требования к разработке автоматизированной обучающей системы в области информационной безопасности // Инженерный вестник Дона, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5596.

10. Ворожцова Т.Н. Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности // Онтология проектирования. 2014. №4 (14). С. 69-77.

References

1. Moskalenko Ju.S. Organizacija sistem, osnovannyh na znanijah [Organization of knowledge-based systems]. Vladivostok: Izdatel'skij dom Dal'nevost. federal. un-ta, 2013. 244 p.

2. Gavrilova T.A., Kudrjavcev D.V., Muromcev D.I. Inzhenerija znanij. Modeli i metody [Knowledge engineering. Models and Methods]. 6-e izd. Saint Petersburg: Lan', 2023. 324 p.

3. Feilmayr C., Wöß W. Data & Knowledge Engineering. 2016. №101. pp. 1-23.

4. Garin M.S., Romanenko E.V. Inzhenernyj vestnik Dona, 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/811.

5. Bubakar I., Bud'ko M.B., Bud'ko M.Ju., Girik A.V. Trudy ISP RAN. 2021, vol. 33. №5. pp. 41-64.

6. Popov M.A., Fedorov D.Ju. Zashhita informacii v komp'juternyh sistemah. 2017. pp. 13-19.

7. Herzog A., Shahmehri N. International Journal of Information Security and Privacy. 2007. №1 (4). pp. 1-23.

8. Miroljubova S.Ju. Monitoring pravoprimenenija. 2022. №1 (42). pp. 39-45.

9. Kolesnikova D.S., Rudnichenko A.K. Inzhenernyj vestnik Dona, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5596.

10. Vorozhcova T.N. Ontologija proektirovanija. 2014. №4 (14). pp. 69-77.