Список цитированных источников

1. Касьяник, В.В. Мобильный помощник водителя в выборе стратегии вождения // Искусственный интеллект. – Донецк: ИПИИ «Наука і освіта». – 2012. – № 3. – С. 253-259.

2. Shuts, Vasili Mobile Autonomous robots – a new type of city public transport / Vasili Shuts, Valery Kasyanik // Transport and Telecommunication. – 2011. – V. 12, No 4. – P. 52-60.

3. Пролиско, Е.Е. Математическая модель работы «ИНФОБУСОВ» / Е.Е. Пролиско, В.Н. Шуть // Матеріали VII-ої Українсько-польскої науково-практычної конференції «Електроніка та інфармаційні технології (ЕлІТ-2015)», 27-30 серпня 2015 р. – Львів-Чинадієво, 2015. – С. 59-62.

4. Шуть, В.Н. Альтернативный метро транспорт на базе мобильных роботов / В.Н. Шуть, Е.Е. Пролиско // Штучний інтелект. – 2016. – № 2 (72). – С. 170-175.

5. Шуть, В.Н. Алгоритм организации городских пассажирских перевозок посредством рельсового беспилотного транспорта "Инфобус" / В.Н. Шуть, Е.В. Швецова // ACTUAL PROBLEMS OF FUNDAMENTAL SCIENCE: third international conference. – Луцк: Вежа-Друк, 2019. – С. 222-226.

6. Shuts, V. Cassette robotized urban transport system of mass conveying passenger based on the unmanned electric cars / V. Shuts, A. Shviatsova// Science. Innovation. Production. Proceedings of the 6th Belarus-Korea Science and Technology Forum. – MINSK: BNTU, 2019. – C. 81-83.

7. Shuts, V. System of urban unmanned passenger vehicle transport / V. Shuts, A. Shviatsova // ICCPT 2019: Current Problems of Transport: Proceedings of the 1st International Scientific Conference. – Ternopol: TNTU, 2019. – C. 172-184.

УДК 004.056.5

Муха А. А.
Научный руководитель: ст. преподаватель Ипатова О. В.

СОСТАВЛЯЮЩИЕ СИСТЕМЫ ЗАЩИТЫ ИНОФРМАЦИИ РЕСПУБЛИКИ БЕЛАРУСЬ

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровень её защиты. При этом необходимость эффективной защиты информации растёт вместе со сложностью архитектуры хранения данных. Необходимость защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы. В Республике Беларусь существует ряд мероприятий в сфере информационной безопасности, среди которых можно выделить такие важные, как: **лицензирование, сертификация, декларирование, экспертиза и аттестация**.

Отношения в области **лицензирования** деятельности по технической и (или) криптографической защите информации в Республике Беларусь регулируются Положением о лицензировании отдельных видов деятельности, утвержденным Указом Президента Республики Беларусь от 1 сентября 2010 г. № 450 «О лицензировании отдельных видов деятельности» (далее – Положение) [1]. Особенности лицензирования деятельности по технической и (или) криптографической защите информации изложены в главе 21 Положения.

Лицензирующим органом, осуществляющим лицензирование деятельности по технической и (или) криптографической защите информации (далее – лицензируемая деятельность), является Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ).

Лицензируемая деятельность осуществляется лишь юридическими лицами Республики Беларусь и включает следующие работы и услуги, указанные в пункте 13 приложения к Положению:

– разработка, производство технических и программных средств обработки информации в защищённом исполнении, технических, программных, программно-аппаратных средств защиты информации и контроля её защищённости, средств криптографической защиты информации;

– проведение специальных исследований технических средств;

– проектирование, создание систем защиты информации на объектах информатизации, предназначенных для проведения работ с использованием государственных секретов;

– проектирование, создание, аттестация систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

– аттестация объектов информатизации, предназначенных для проведения работ с использованием государственных секретов;

– проектирование, создание аудит-систем информационной безопасности критически важных объектов информатизации;

– проведение работ по выявлению специальных технических средств, предназначенных для негласного получения информации;

– удостоверение формы внешнего представления электронного документа на бумажном носителе;

– оказание услуг по распространению открытых ключей проверки электронной цифровой подписи.

Под информацией, для осуществления деятельности по технической и (или) криптографической защите которой требуется получение лицензии, понимается информация: распространение и (или) предоставление которой ограничено; обрабатываемая на критически важных объектах информатизации; обрабатываемая в информационных системах в форме электронных документов.

Не требуется получения лицензии для выполнения работ по технической и (или) криптографической защите информации, если эти работы выполняются *для собственных нужд* обладателем информации, распространение и (или) предоставление которой ограничено, собственником (владельцем) информационных систем и критически важных объектов информатизации.

Лицензируемая деятельность осуществляется только государственными юридическими лицами Республики Беларусь и хозяйственными обществами, 100 процентов акций (долей в уставных фондах) которых принадлежат Республике Беларусь, по следующим составляющим её работам и (или) услугам:

– аттестация объектов информатизации, предназначенных для проведения работ с использованием государственных секретов, если владельцем соответствующего объекта информатизации является государственный орган или государственная организация, а также хозяйственное общество, 50 и более процентов акций (долей в уставном фонде) которого находится в собственности Республики Беларусь и (или) её административно-территориальных единиц;

– проведение работ по выявлению специальных технических средств, предназначенных для негласного получения информации.

Перед выпуском в обращение на рынке средства защиты информации должны быть подвергнуты процедуре подтверждения соответствия требовани-

ям информационной безопасности технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность», утверждённый постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 (далее – ТР 2013/027/BY), вступившего в силу 1 января 2014 г. [2]. Согласно регламенту устанавливается две формы подтверждения соответствия: в форме **сертификации и декларирования соответствия.**

Технологии защиты информации и информационной безопасности идут следом за информационными технологиями. Все чаще мы должны обеспечить защищённость информационных продуктов и систем зарубежного производства, о которых нам известны только их потребительские характеристики. Упомянутый выше регламент устанавливает базовые требования информационной безопасности к средствам защиты информации. Потребительские функции средств защиты информации определяются в зависимости от назначения и условий эксплуатации объекта защиты. Как правило, показатели и нормы защищённости информации закрепляются на национальном уровне. В связи с этим требования к функциям защиты средств защиты информации устанавливаются в национальных стандартах.

Подтверждению соответствия требованиям информационной безопасности технического регламента *путём сертификации* подлежат средства защиты информации, которые будут использоваться для: технической защиты *государственных секретов*; создания систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой *ограничено*; создания систем безопасности *критически важных объектов* информатизации; обеспечения целостности и подлинности *электронных документов* в *государственных информационных системах* [2, п. 3]. *В остальных случаях* подтверждение соответствия средств защиты информации требованиям информационной безопасности технического регламента ТР 2013/027/BY проводится *путём декларирования соответствия* [2, п. 4].

Соответствие средств защиты информации ТР 2013/027/BY обеспечивается выполнением требований информационной безопасности технического регламента непосредственно либо выполнением требований госстандартов, определённых приказом ОАЦ от 17 декабря 2013 г. № 94 «О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY» [3].

Срок действия сертификата соответствия при сертификации серийно выпускаемой продукции – 5 лет. В случае сертификации партии продукции – сертификат соответствия выдается на время срока годности продукции либо её реализации или без ограничения срока при возможности однозначной идентификации каждой единицы сертифицированной продукции [4, п. 23.3]. Хранение же документов проверки должно осуществляться в течение не менее 10 лет со дня снятия с производства средств защиты информации (изготовителем) или со дня реализации последнего изделия из партии (импортёром) [2, п. 10].

В соответствии с Законом Республики Беларусь «Об информации, информатизации и защите информации» 2008 г. [5] для создания системы защиты информации используются средства защиты информации, имеющие *сертификат соответствия,* выданный в Национальной системе подтверждения

соответствия Республики Беларусь, или *положительное экспертное заключение по результатам* **государственной экспертизы**, порядок проведения которой определяется Положением о порядке проведения государственной экспертизы средств технической и криптографической защиты информации, утверждённое приказом ОАЦ от 26 августа 2013 г. № 60 [6].

В соответствии с пунктом 2 Положения о экспертизе государственная экспертиза (далее – экспертиза) средств технической и криптографической защиты информации (далее – продукция) – оценка соответствия продукции *требованиям* по технической и криптографической защите информации, которые *техническими нормативными правовыми актами Республики Беларусь не установлены*, в целях подготовки экспертного заключения по использованию (применению) данной продукции [6, п. 2]. Объектами экспертизы выступают средства технической и криптографической защиты информации, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов. Экспертиза продукции проводится ОАЦ по инициативе заявителя.

Экспертиза средств криптографической защиты информации проводится на соответствие требованиям по криптографической защите информации, содержащимся *в документации изготовителя и (или) определяемым органом государственной экспертизы* [6, п. 4]. При этом для проведения экспертизы средств *криптографической защиты информации заявитель по согласованию с органом государственной экспертизы определяет требования*, на соответствие которым проводится экспертиза [6, п. 5]. Срок действия **экспертного заключения** на продукцию составляет: для средств криптографической защиты информации – 5 лет; для средств технической защиты информации – 2 года [6, п. 32].

Аттестация систем защиты информации проводится в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утверждённым ОАЦ 30 августа 2013 г. № 62 [7]. Под аттестацией системы защиты информации информационной системы (далее – аттестация) понимается комплекс организационно-технических мероприятий, в результате которых документально *подтверждается соответствие требованиям законодательства* об информации, информатизации и защите информации, в частности, требованиям по защите информации от утечки по техническим каналам [7, п. 2].

Аттестацию систем защиты информации проводят организации, имеющие соответствующее специальное разрешение (лицензию) ОАЦ. Собственники (владельцы) информационных систем, имеющие в своём составе *подразделения технической защиты информации* или иные подразделения (должностных лиц), выполняющие функции по технической и (или) криптографической защите информации, *вправе самостоятельно проводить аттестацию* систем защиты информации этих информационных систем [7, п. 3]. 7. *Наличие аттестата* соответствия является *обязательным условием* для обработки информации, распространение и (или) предоставление которой ограничено в течение установленного в нем срока [7, п. 7].

Аттестация вновь создаваемой системы защиты информации осуществляется *до ввода информационной системы в эксплуатацию* [7, п. 6]. В связи с

тем, что аттестация проводится до ввода системы в эксплуатацию, допускается ввод объекта в опытную эксплуатацию. Основанием для эксплуатации информационной системы является наличие аттестата соответствия требованиям по защите информации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемых объектов *в реальных условиях эксплуатации* информационной системы с целью оценки соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации [7, п. 8]. К аттестуемым объектам информатизации относятся: системы защиты информации; выделенные помещения, предназначенные для ведения секретных переговоров или в которых находятся средства конфиденциальной телефонной связи; средства вычислительной техники, используемые для обработки информации, отнесенной к государственным секретам.

Законодательством Республики Беларусь предусмотрено достаточно большое число процедур по защите информации, среди которых: лицензирование деятельности по технической и (или) криптографической защите информации (не требуется получения лицензии для выполнения работ по данной защите информации для собственных нужд), сертификация средств защиты наиболее важной информации (государственных секретов, электронных документов, критически важных объектов информатизации; информации государственных информационных систем; информации, распространение и предоставление которой ограничено; в остальных случаях – декларирование соответствия), проведение государственной экспертизы (в отношении защиты продукции, требования к которой техническими нормативными правовыми актами не установлены), аттестация средств защиты информации и иных объектов информатизации в реальных условиях перед вводом в эксплуатацию на самом предприятии, организации.

Список цитированных источников

1. Положение о лицензировании отдельных видов деятельности [Электронный ресурс] : утв. Указом Президента Респ. Беларусь, 1 сент. 2010 г., № 450 : в ред. от 31 дек. 2019 г. № 499// Эталон-Беларусь / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2020.

2. Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) [Электронный ресурс] : утв. пост. Совета Министров Респ. Беларусь, 15 мая 2013 г., № 375 // Эталон-Беларусь / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2020.

3. О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 17 дек. 2013 г. № 94 : в ред. от 30 марта 2018 г. № 41 // Эталон-Беларусь / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2020.

4. Единый перечень административных процедур, осуществляемых государственными органами и иными организациями в отношении юридических лиц и индивидуальных предпринимателей [Электронный ресурс] : утв. пост. Совета Министров Респ. Беларусь от 17 февр. 2012 г. № 156 6 в ред. от 24 апр. 2020 г. № 254 // Эталон-Беларусь / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2020.

5. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь от 10 нояб. 2008 г., № 455-З : в ред. от 11 мая 2016 г. № 362-З // Эталон-Беларусь / Нац. цент правовой ин-форм. Респ. Беларусь. – Минск, 2020.

6. Положение о порядке проведения государственной экспертизы средств технической и криптографической защиты информации [Электронный ресурс] : утв. приказом Оперативно-аналитического центра при Президенте Респ. Беларусь от 26 авг. 2013 г. № 60 : в ред. от // Эталон-Беларусь / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2020.

7. Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам [Электронный ресурс] : утв. приказом Оперативно-аналитического центра при Президенте Респ. Беларусь, 30 авг. 2013 г. № 62 : в ред. от 11 октября 2017 г. № 64 // Эталон-Беларусь / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2020.

УДК 004.89

Мычко Н. А.
Научный руководитель: к.т.н., доцент Крапивин Ю. Б.

МЕТОДЫ АВТОМАТИЗАЦИИ ОБРАБОТКИ ТЕКСТОВЫХ ОБРАЩЕНИЙ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Увеличение использования технологий в современности приводит к росту требований к обеспечению службы технической поддержки (далее – СТП). Техническая поддержка часто подразделяется на уровни с целью улучшения обслуживания организации или базы клиентов. Количество уровней определяется потребностями и желаниями бизнеса или же ставится в зависимость от возможностей эффективно помочь клиентам или пользователям [1].

В свою очередь высокая скорость роста количества пользователей в той или иной сфере вынуждает совершенствовать способы обработки обращений, реализовывать частичную или полную автоматизацию этих процессов. Легко заметить, что основным и наиболее востребованным способом представления информации является текст на естественном языке. Именно поэтому далее речь пойдёт об обработке подобных обращений [2].

Обобщенное представление процесса автоматического анализа текста в контексте практически любой задачи, связанной с автоматизацией обработки текстовых сообщений, схематично может быть представлено на различных уровнях, например так, как это сделано на рисунке 1.

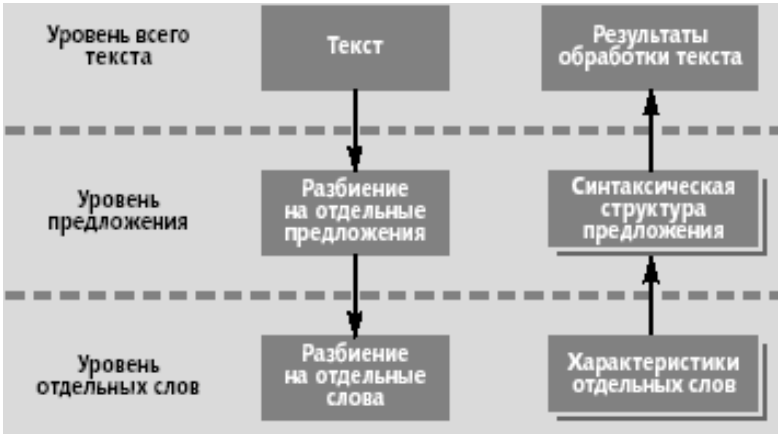

Рисунок 1 – Уровни автоматического анализа текста