УДК 004.91:004.056.53

КРИТЕРИАЛЬНАЯ СИСТЕМА ОЦЕНКИ ЗАЩИЩЕННОСТИ ДОКУМЕНТОВ НА ОСНОВЕ ТЕХНОЛОГИИ ЛЕКСИКОЛОГИЧЕСКОГО СИНТЕЗА

[1,2]Черников Б.В., [2]Трофимова А.В.

[1]ООО «Газпром ВНИИГАЗ», e-mail: bor-cher@yandex.ru;

[2]РЭУ им. Г.В. Плеханова, Москва, e-mail: 13goan@gmail.com

Необходимость защиты информации определяется не только потребностью организаций сохранять конфиденциальность коммерческой тайны для сохранения конкурентоспособности, но и законодательными актами, описывающими требования защиты персональных данных и другой конфиденциальной информации. Обеспечение безопасности такой информации требует комплексного подхода: защиты на организационно-правовом и техническом направлениях. Организационные меры являются основополагающими в данной сфере, но не покрывают полный спектр угроз. Например, при передаче электронных документов по каналам связи существует вероятность ее перехвата с помощью применения технических средств. Защита информации от подобной угрозы осуществляется посредством применения специальных методов – шифрования и кодирования. Аналогичным способом обеспечения конфиденциальности передаваемой информации является технология защиты электронных документов на основе лексикологического синтеза. Основой данной технологии является автоматизированное создание документов, в ходе которого формируется индексная последовательность, которая и передается по каналу связи. Выбор одного из методов защиты информации должен опираться на некие признаки, позволяющие оценить вероятность достижения цели выбора. В работе предложены критерии для сравнения методов защиты информации при передаче электронных документов по каналу связи в рамках двух групп – критерии, связанные с надежностью обеспечения безопасности информации, и критерии, связанные с организацией защиты конфиденциальных данных. Сформированные критерии позволяют сравнить рассматриваемые методы защиты данных. В результате исследования проведен анализ технологии защиты документов на основе лексикологического синтеза в сравнении с шифрованием и кодированием, который показал, что сформированная критериальная система требует расширения значимых компонентов, сделан вывод о различии сравниваемых методов защиты информации в аспекте эффективности.

Ключевые слова: электронный документ, защита информации, конфиденциальность, лексикологический синтез, критерий, шифрование

CRITERION SYSTEM FOR ASSESSING THE SECURITY OF DOCUMENTS BASED ON LEXICOLOGICAL SYNTHESIS TECHNOLOGY

[1,2]Chernikov B.V., [2]Trofimova A.V.

[1]OOO «Gazprom VNNIGAZ», e-mail: bor-cher@yandex.ru;

[2]Plekhanov Russian University of Economics, Moscow, e-mail: 13goan@gmail.com

The need to protect information is determined not only by the need of organizations to maintain confidentiality of commercial secrets in order to maintain competitiveness, but also by legislative acts describing the requirements for the protection of personal data and other confidential information. Ensuring the security of such information requires an integrated approach – protection in the organizational, legal and technical areas. Organizational measures are fundamental in this area, but do not cover the full range of threats. For example, when transmitting electronic documents via communication channels, there is a possibility of its interception by using technical means. Information is protected against such a threat by applying special methods – encryption and encoding. A similar way to ensure the confidentiality of information transmitted is the technology of protecting electronic documents based on lexicological synthesis. The basis of this technology is the automated creation of documents, during which an index sequence is formed, which is transmitted via a communication channel. The choice of one of the methods of information protection should be based on certain signs, allowing to assess the probability of achieving the goal of choice. The paper proposed criteria for comparing information protection methods for transmitting electronic documents via a communication channel within two groups – criteria related to the reliability of information security, and criteria related to the organization of the protection of confidential data. Formed criteria allow us to compare the data protection methods under consideration. The study resulted in a comparative analysis of the document protection technology based on lexicological synthesis, encryption and coding, which showed that the obtained criterion system requires expanding the components, and it was also concluded that there are differences between the compared information protection methods.

Keywords: electronic document, information security, confidentiality, lexicological synthesis, criterion, encryption

Информационная безопасность в широком смысле представляет собой совокупность средств защиты информации от случайного или преднамеренного воздействия. Независимо от причины воздействия (причины искусственного характера или естественные факторы) владелец информации может получить ущерб.

Потенциально возможное влияние или воздействие на информацию с последующим нанесением убытка чьим-то потребностям является угрозой информации [1]. Угрозы информационной безопасности проявляются не самостоятельно, а через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть

через уязвимости. Угроза приводит к нарушению деятельности систем на конкретном объекте-носителе, что может повлиять на соблюдение конфиденциальности информации. Нарушение конфиденциальности информации часто ведет к материальному ущербу, например, при разглашении «ноу-хау» компания несет финансовые потери, а также нематериальные – потеря репутации, снижение доверия.

Защита конфиденциальной информации обеспечивается комплексом мер, направленных на противодействие злоумышленнику – лицу, принимающему преднамеренные действия для доступа к информации [2]. В качестве таких мер могут выступать:

– препятствие на пути нарушителя – физическими (например, ограничение доступа с помощью металлических дверей) и программными средствами (для этих целей применяется авторизация пользователя при входе во многие программные комплексы);

– маскировка или преобразование данных;

– разработка нормативно-правовых актов, направленных на побуждение пользователей к должному поведению (к этому способу можно отнести подписание обязательства о неразглашении служебных сведений).

Меры должны использоваться в комплексе, так как каждая их группа перекрывает ограниченный набор угроз. Работу сотрудников с конфиденциальными данными можно регламентировать локальными нормативными актами, однако такие меры защиты не учитывают угрозы технического характера, например попытки удаленного перехвата информации, соответственно, при передаче электронных документов необходимо обеспечить защиту информации на техническом уровне. В данном случае основным методом безопасности является криптографическая защита. Конфиденциальность обеспечивается путем преобразования открытого теста при помощи алгоритма, называемого шифром. При использовании данного метода защищен сам документ с текстом, а не доступ к нему. Для аналогичной цели предназначена и защита информации при формировании документов на основе технологии автоматизированного лексикологического синтеза (ЛЛС). Достоинства этого метода защиты информации описываются в данном исследовании.

Каждый из методов защиты информации реализуется при помощи различных категорий средств. Основные средства – организационные и технические. Определение необходимых методов требует ответа на вопросы: «Что защищается?», «От чего защищается?», «Какими средствами защищается?» Для выбора метода или средства защиты исходя из конкретной ситуации формируются критерии сравнения.

Во избежание получения материального и иного ущерба, который может привести к тяжелым последствиям (вплоть до банкротства компании или угрозы жизни и здоровью человека) вследствие хищения конфиденциальных данных, следует обеспечивать их безопасность. Защита конфиденциальной информации – это совокупность мероприятий, направленных на обеспечение сохранности информации от несанкционированного доступа. Согласно законодательству, в целях защиты, например, персональных данных необходимо использовать комплекс мер, включая организационные и технические [3]. Организационные меры защиты информации определяются нормативно-правовыми документами, в которых учитываются сфера деятельности и особенности функционирования организаций. При использовании технических мер необходимо осуществить выбор в пользу того или иного метода защиты. Принятие оптимального решения требует соответствия определенным критериям, в соответствии с которыми будут оцениваться альтернативные варианты. Определение критериев – ключевой момент при выборе метода защиты информации, так как анализ возможных решений с помощью критериальной системы покажет для лица, принимающего решение, преимущества и недостатки выбираемого метода, его соответствие цели.

Цель исследования: формирование комплекса критериев для сравнения методов защиты информации с методом защиты документов на основе лексикологического синтеза при передаче электронных документов по каналам связи

Организационно-правовая основа защиты информации

Категория мер обеспечения информационной безопасности на основе нормативных документов представлена законодательными актами и нормативно-распорядительными документами, которые действуют в масштабах государства или на уровне организации.

В мировой практике при разработке нормативных актов ориентируются на стандарты защиты информационной безопасности, основным в настоящее время считается стандарт ISO/IEC 27000, включающий в себя целое семейство нормативных документов. Стандарт создавали две организации:

− ISO – Международная организация по стандартизации, которая разрабатывает и утверждает большинство признанных на международном уровне методик серти-

фикации качества процессов производства и управления;

– IEC – Международная некоммерческая организация по стандартизации в области электрических, электронных и смежных технологий. Некоторые из стандартов МЭК разрабатываются совместно с Международной организацией по стандартизации.

Актуальная версия стандарта ISO/IEC 27000-2016 предлагает готовые рекомендации, необходимые для управления информационной безопасностью.

В качестве нормативных актов на уровне компании разрабатываются перечни сведений, составляющих коммерческую тайну, приложения к трудовым договорам, закрепляющие ответственность за разглашение конфиденциальных данных, внутренние стандарты и методики. Внутренние нормы и правила должны содержать описание механизмов реализации защиты информации и меры ответственности. Чаще всего меры носят дисциплинарный характер, и нарушитель должен быть готов к тому, что за нарушением режима коммерческой тайны могут последовать организационные санкции вплоть до увольнения.

В рамках административной деятельности по обеспечению информационной безопасности для сотрудников служб безопасности организаций доступен широкий набор действий. Это и архитектурно-планировочные решения, позволяющие защитить переговорные комнаты и кабинеты руководства от прослушивания, и установление различных уровней доступа к информации. К важным организационным мерам следует отнести сертификацию деятельности компании по стандартам ISO/IEC 27000, сертификацию отдельных аппаратно-программных комплексов, аттестацию субъектов и объектов на соответствие необходимым требованиям безопасности, получение лицензий, необходимых для работы с защищенными массивами информации.

С точки зрения регламентации деятельности персонала необходимо оформление системы запросов на допуск к интернету, внешней электронной почте, другим ресурсам. Дополнительным элементом является получение электронной подписи для усиления безопасности финансовой и другой информации, которую передают государственным органам по каналам связи посредством, например, электронной почты.

Морально-этические меры определяют личное отношение человека к конфиденциальной информации. Повышение уровня знаний сотрудников касательно влияния угроз на деятельность компании влияет на степень сознательности и ответственности сотрудников.

В работе [4] отмечается, что защита информации требует комплексного подхода. В совокупности с организационно-правовыми мерами необходимо использовать и технические.

Технические меры защиты

Физические средства – это механические, электрические, электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним [5]. Замки, в том числе электронные, экраны, жалюзи призваны создавать препятствия для контакта дестабилизирующих факторов с системами. Группа этих мер дополняется средствами систем промышленной безопасности, например, видеокамерами, видеорегистраторами, датчиками, выявляющие движение или превышение степени электромагнитного излучения в зоне расположения технических средств снятия информации, закладных устройств.

Аппаратные средства – это электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в информационные и телекоммуникационные системы [6]. Программные средства – это прикладные, системные и комплексные программы, предназначенные для решения задач, связанных с обеспечением безопасности информации.

К дополнительным средствам обеспечения информационной безопасности относятся различные криптографические алгоритмы, реализующиеся в качестве программных и программно-аппаратных средств, позволяющие шифровать информацию при хранении и перенаправляемую по внешним каналам связи. При передаче данных по каналам связи наиболее распространенным методом защиты является шифрование содержимого документа. Менее популярным аналогом в целях защиты данных является кодирование – замена элементов текста на различные символы в соответствии с таблицей кодировки.

Все средства, обеспечивающие безопасность информации, должны использоваться в совокупности, после предварительной оценки ценности информации и сравнения ее со стоимостью ресурсов, затраченных на охрану.

Защита документов на основе лексикологического синтеза

Аналогом криптографии, как методу защиты информации при передаче документов по каналам связи, является защита электронных документов на основе технологии лексикологического синтеза.

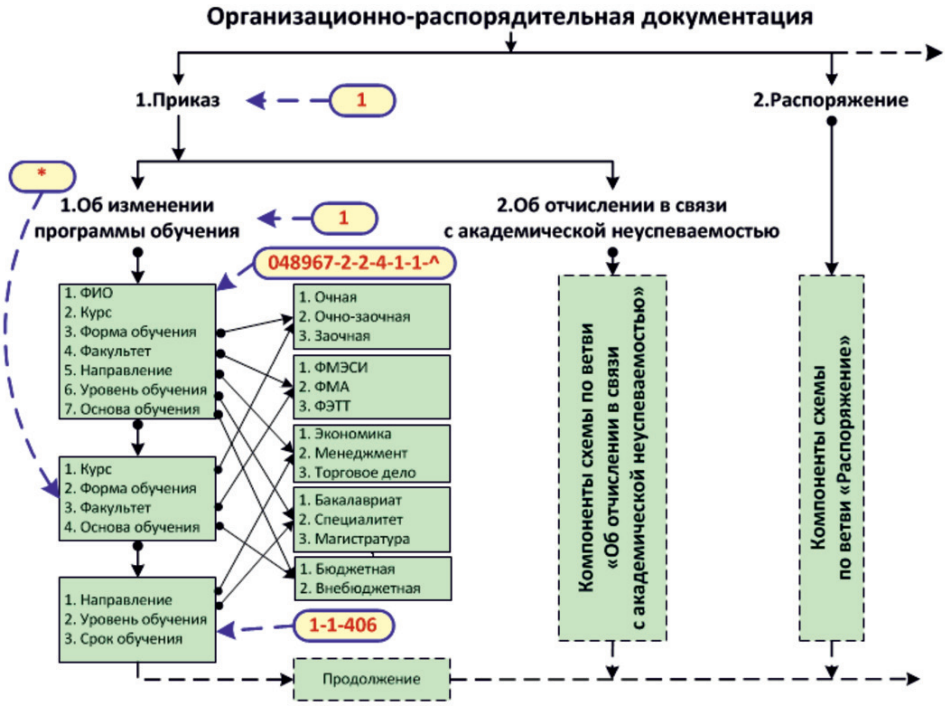

Рис. 1. Фрагмент лексикологической схемы организационно-распорядительной документации вуза

Данный метод дополняет процесс создания электронных документов в автоматизированном режиме [7]. Формируется набор унифицированных по форме и содержанию документов. Каждый такой документ состоит из опорных слов и соответствующих им формулировок. Данный массив информации складывается в специализированную базу знаний. Опорные слова образуют лексонтологию – лексикологическую схему документа. Пример такой схемы представлен на рис. 1.

Вся информация в документе делится на четыре категории [7]:

– унифицированная постоянная (редко меняющаяся информация, например тип документа или наименование организации);

– унифицированная переменная (возможно представление в качестве справочника: перечень факультетов, форм обучения и т.д.);

– переменная вводимая (имеет определенный формат представления данных, конкретизирующие данные для конкретного экземпляра – табличные данные, сведения о программе обучения в часах);

– неунифицированная (свободные формулировки).

При создании конкретного экземпляра документа выбираются опорные слова, которым соответствуют определенные текстовые фрагменты, внедряемые в документ. Важно отметить, что форма документа также закладывается в базу знаний и выбирается на начальном этапе создания документа.

Сущность защиты конфиденциальной информации заключается в следующем [7]. В процессе формирования документа на основе лексикологического синтеза фиксируются индексы, соответствующие каждому опорному слову на лексикологической схеме (рис. 1). Совокупность данных индексов составляет индексную последовательность. Отличие описываемого метода защиты информации от шифрования заключается в том, что по каналу связи передается не сам документ, а сформированная индексная последовательность.

Индексная последовательность содержит следующие элементы:

– индекс формы (типа) документа;

– индекс заголовка документа;

– индексы опорных слов;

– зашифрованные свободные формулировки;

– индекс электронной подписи.

Пример индексной последовательности, сформированной на основе фрагмента лексикологической схемы организационно-распорядительной документации вуза (рис. 1):

1:1:048067-2-2-4-1-1-^:*:1-1-406,

где уровни уточнения информации разделяются знаком «:», внутриуровневое разделе-

ние обозначается символом «–», отсутствие уточняющей информации на уровне «*», отсутствие информации внутри уровня – «^».

Для приведенного на рис. 1 примера первому уровню присваивается индекс 1, которому соответствует вид документа «Приказ», второму уровню – индекс 2 с соответствующим заголовком «Об изменении программы обучения», третьему – код студента 048967, 2 курс, очно-заочная форма обучения с индексом 2, факультет – 4, направление – 1, уровень обучения – 1. Основа обучения не выбирается, следовательно, ставится знак «^». Четвертый уровень не уточняется, указывается знак «*». Пятому уровню соответствуют индексы направления – 1, уровня обучения – 1 и срока обучения – 406.

Процесс обмена документами с применением технологии лексикологического синтеза осуществляется следующим образом. На стороне отправителя формируется информационная посылка, содержащая индексную последовательность, которая и отправляется по каналу связи. На стороне получателя после получения данной посылки происходит автоматическое восстановление документа путем определения по индексам опорных слов и соответствующих им формулировок по лексикологической схеме. Данная технология работает только при наличии у обеих сторон согласованной лексикологической схемы, без которой создание и последующее восстановление документа невозможны [7].

Критерии для сравнения технических методов защиты информации с защитой документов на основе лексикологического синтеза

Методы защиты информации, изложенные выше, имеют свои достоинства и недостатки. Для того чтобы определить подходящий метод в конкретной ситуации, необходимы некие признаки для сравнения.

Критерий – признак, на основании которого производится оценка, определение или классификация чего-либо [8]. Критерии могут измеряться числовыми оценками и нечеткими множествами. При определении критериев для выбора метода защиты информации важно корректно поставить задачу, так как при разных целях принятия решения требуются различные критерии. Цель в рамках данного исследования сформулирована следующим образом. Необходимо сформировать критерии для сравнения метода защиты электронных документов на основе лексикологического синтеза с аналогичными техническими методами при передаче документов по каналам связи.

Подбор критериев можно разделить на два типа:

− критерии, отражающие степень защиты информации;

− критерии, связанные с организацией защиты и процесса передачи информации.

Чтобы метод считался конкурентоспособным, он обязательно должен поддерживать основные свойства информации – целостность, доступность, конфиденциальность [9]. К данным свойствам следует добавить неотказуемость, то есть неотрекаемость от авторства информации. Кроме того, целесообразно учесть такие критерии, как возможность восстановления исходного текста при перехвате и влияние знания алгоритма защиты на возможность восстановления текста. Данные признаки важны при передаче конфиденциальной информации по каналам связи.

К дополнительным критериям относятся:

− передача самого документа, т.е. критерий определяет, передается ли документ, содержащий конфиденциальный текст, или передаче подлежит только текст (содержание документа);

− является частью документооборота или отдельным средством, т.е. является ли реализация метода защиты в отношении системы электронного документа оборота как встроенное или отдельное средство;

− определение ошибки при получении – фиксация результатов передачи данных и журнала ошибок, доступных для администратора системы;

− дополнительные аппаратные средства – требование к дополнительным аппаратным средствам (за исключением аппаратуры, на которой используется система электронного документооборота или обычное создание документов) при реализации метода;

− использование при обмене неунифицированными документами, т.е. целесообразность использования метода защиты при обмене документами, которые сложно унифицировать по форме и содержанию.

Скорость передачи информации по каналу связи не рассматривается, так как в современном мире данные показатели будут незначительны при выборе метода защиты.

Часть описанных критериев принимает значения «да/возможно/нет», для рейтинговой оценки можно представить значения как «2/1/0» соответственно. В целях удобства сравнения методов в совокупности для остальных критериев в табл. 1 приведены такие же диапазоны значений. Для лица, принимающего решение о выборе метода защиты информации, важно определить веса критериев – важность критерия при приня-

тии решения. Вес, как правило, определяется экспертным путем. Исходя из развития информационных технологий, приведен пример расставленных весов сформированных критериев, причем сумма весов критериев должна равняться единице (табл. 1).

В каждом отдельном случае принятия решения веса критериев определяются, как правило, лицом, принимающим это решение. В данном исследовании веса приведены для примера. Наибольший вес распределяется на концептуальный подход к документообороту – используется ли он для формирования и обмена унифицированными документами, что сразу может отсечь некоторые варианты при выборе. Цель данных методов – защита информации, соответственно, следующим шагом вес получают критерии, связанные непосредственно с обеспечением безопасности данных, такие как свойства информации, которое обеспечивает метод, возможность восстановления исходного текста при перехвате и влияние знания алгоритма защиты на возможность восстановления текста. Определение ошибки при передаче также получает вес 0,1, так как при передаче документов важно определять, дошла ли информация до получателя и с каким результатом, что позволяется предпринять действия по устранению ошибок. Дополнительными критериями являются необходимость в дополнительных аппаратных средствах и передача самого документа по каналу связи, значения которые не сказываются критично на защите информации, веса распределяются для них в последнюю очередь.

Сравнение методов по выработанным критериям

В табл. 2 приведены показатели для таких методов защиты информации, как шифрование, кодирование и защита документов на основе лексикологического синтеза.

По критериям, приведенным в табл. 2, определить однозначно, какой метод следует использовать при поставленной цели, сложно. Некоторые критерии не дают понять разницы, особенно когда все методы принимают одинаковое значение. Сравнение показывает, что по критериям, отражающим защиту информации, описываемые методы приблизительно равноценны (рис. 2), но важным отличием являются значения критерия «Передача самого документа», так как защита на основе лексикологического синтеза позволяет не передавать сам документ и определять форму со всеми сопутствующими атрибутами на стороне получателя.

Определение наилучшего метода защиты согласно критериям (табл. 2) осуществляется через общий показатель (ОП) для каждого метода, считаемый по формуле

$$\text{ОП} = \sum_{k=1}^{n} З * В,$$

где З – значение критерия, В – вес критерия, n – количество критериев. Общий показатель учитывает важность критерия для лица, принимающего решение, а также значение самого критерия в совокупности. Применив данную формулу к табл. 2, получаются следующие показатели (табл. 3).

Таблица 1

Веса критериев для выбора метода защиты информации при передаче по каналам связи

№ п/п	Критерий	Возможные значения	Вес
1	Свойства информации, которые обеспечивает метод	Целостность, доступность и конфиденциальность, неотказуемость	0,2
2	Возможность восстановления исходного текста при перехвате	Шкала от 0 до 2, где 2 – минимальная вероятность восстановления, 0 – максимальная вероятность восстановления	0,1
3	Влияние знания алгоритма защиты на возможность восстановления текста	Шкала от 0 до 2, где 2 – минимальное влияние, 0 – максимальное влияние	0,1
4	Передача самого документа	Шкала от 0 до 2, где 2 – документ не передается, 0 – передается	0,1
5	Определение ошибки при получении	Шкала от 0 до 2, где 2 – да, 1 – возможно, 0 – нет	0,1
6	Необходимость в дополнительных аппаратных средствах	Шкала от 0 до 2, где 2 – нет, 1 – возможно, 0 – да	0,1
7	Использование при неунифицированном документообороте	Шкала от 0 до 2, где 2 – да, 1 – возможно, 0 – нет	0,2

Таблица 2

Сравнительная таблица методов защиты информации при передаче по каналам связи

№ п/п	Критерий	Методы		
		ЛЛС	Шифрование	Кодирование
1	Принцип, на обеспечение которого направлена защита	Конфиденциальность Неотказуемость	Конфиденциальность Неотказуемость	Конфиденциальность
2	Возможность восстановления исходного текста при перехвате	2	2	1
3	Влияние знания алгоритма защиты на возможность восстановления текста	2	2	1
4	Передача самого документа	2	0	0
5	Определение ошибки при получении	2	2	2
6	Необходимость в дополнительных аппаратных средствах	2	1	2
7	Использование при неунифицированном документообороте	1	2	2

Таблица 3

Общие показатели сравнения методов защиты информации

№ п/п	Метод защиты информации	Общий показатель
1	ЛЛС	1,2
2	Шифрование	1,1
3	Кодирование	1

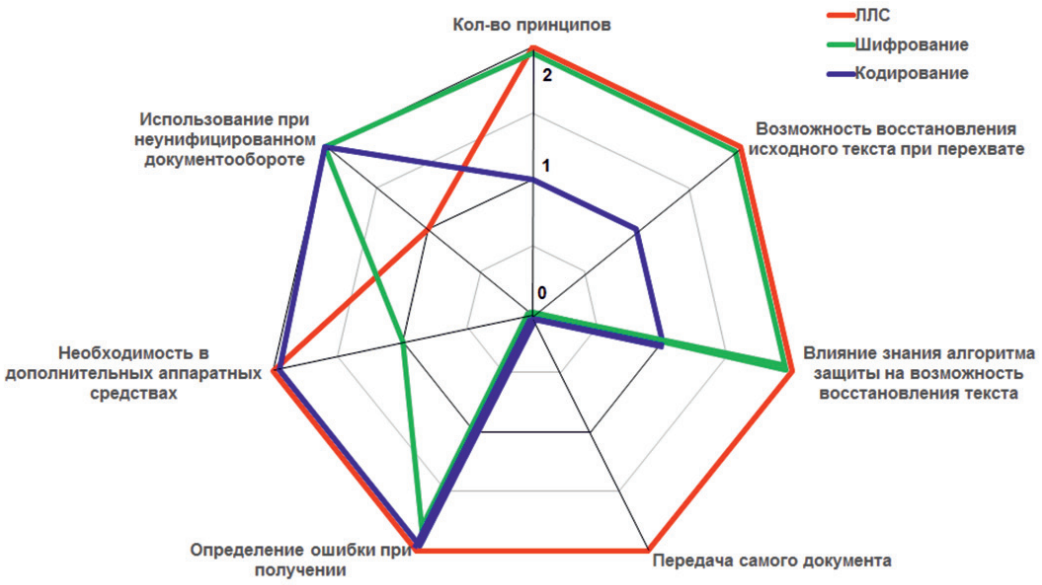

Рис. 2. Лепестковая диаграмма параметрического сравнения методов защиты документов при передаче по каналам связи

Согласно расставленным весам и значениям критериев наибольший общий показатель имеет метод защиты информации на основе лексикологического синтеза.

Выбор метода может определяться на основе того, является ли целью защиты документооборот унифицированных документов, так как реализация защиты документов на основе лексикологического синтеза может быть проще установки средств криптографической защиты данных. Кроме того, во многих случаях имеет весомое значение ценовая политика организации в отношении обеспечения информационной безопасности. Тем не менее, если судить в комплексе в целом, технико-экономиче-

ские показатели лексикологического синтеза можно считать более выгодными даже по причине меньшей необходимости в дополнительном обеспечении какими-либо средствами поддержки защиты информации передаваемых документов.

Заключение

1. Целостность, доступность и конфиденциальность информации обеспечиваются комплексом мер различной направленности: организационные, правовые, технические. Каждое из перечисленных направлений защищает от своего спектра угроз. Определение метода защиты зависит от поставленной цели.

2. В процессе исследования анализировались методы защиты информации при передаче электронных документов по каналам связи: шифрование, кодирование и защита документов на основе лексикологического синтеза. Исходя из особенностей данных методов сформирован перечень критериев для сравнения.

3. Сформированные критерии показали, что в отношении информационной безопасности защита на основе лексикологического синтеза и шифрование во многом равноценны. Выбор одного из данных методов должен опираться на уже сформированную инфраструктуру в организации, поддерживающую обмен электронными документами, так как в случае отсутствия системы электронного документооборота можно реализовать автоматизированное создание документов на основе лексикологического синтеза с параллельным процессом формирования индексной последовательности. Такое решение проще установки раздельных систем документооборота и, дополнительно, криптографической защиты данных, что, безусловно, обеспечивает определенный экономический выигрыш.

Список литературы

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М.: СТАНДАРТИНФОРМ, 2007. 8 с.

2. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М.: СТАНДАРТИНФОРМ, 2014. 106 с.

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Российская газета. Федеральный выпуск № 4131 (0). 2006.

4. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. М.: МГТУ им. Н.Э. Баумана, 2016. 252 с.

5. Беляев М.А., Лысенко В.В., Малинина Л.А. Основы информатики. Ростов н/Д.: Феникс, 2006. 352 с.

6. Нестеров С.А. Основы информационной безопасности: учебное пособие. 5-ое изд., стер. СПб.: Лань, 2019. 324 с.

7. Трофимова А.В., Черников Б.В. Об индексной последовательности при защите документов на основе лексикологического синтеза // Современные наукоемкие технологии. 2018. № 6. С. 150–156.

8. Ефремова Т.Ф. Современный толковый словарь русского языка. Т. 1. СПб.: Астрель, 2006, 1168 с.

9. Крылов Г.О., Ларионова С.Л., Бекетова Ю.М. Международные основы и стандарты информационной безопасности финансово-экономических систем. М.: Прометей, 2018. 174 с.

10. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. СПб.: Питер, 2017. 256 с.

11. Черников Б.В. Способ автоматизированного лексикологического синтеза документов с защищенной информацией при передаче их по каналам связи. Патент РФ № 2331104. 2008.