УДК 004.02:004.056

НАПРАВЛЕНИЯ РАЗВИТИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СОВРЕМЕННЫХ УСЛОВИЯХ

[1,2]Жигалов К.Ю., [2]Подлевских А.П., [3]Аветисян К.Р.

[1]Институт проблем управления им. В.А. Трапезникова РАН, Москва, e-mail: kshakalov@mail.ru;
[2]НОУ ВО «Московский технологический институт», Москва, e-mail: kshakalov@mail.ru;
[3]ФГКОУ ВО «Московский университет МВД России имени В.Я. Кикотя», Москва, e-mail: Karen-Avetisyan-1989@bk.ru

В настоящее время электронный документооборот набирает свою популярность, его можно встретить не только в отдельно взятых организациях, но и на различного рода взаимодействиях между структурами и организациями (электронное правительство). Последний аспект позволяет с уверенностью говорить о необходимости развития систем обеспечения безопасности электронного документооборота в современных условиях. Основное внимание в статье уделяется рассмотрению основ и принципов построения систем документооборота для небольших и средних организаций. Перечислены задачи защиты системы электронного документооборота и требования к системе, выдвигаемые для обеспечения ее безопасности. На основе комплексного анализа существующих систем и методов защиты выработаны основные направления развития данного рода систем. Предложенные направления развития систем обеспечения безопасности электронного документооборота, при их одновременной реализации, позволят повысить эффективность защиты как самих систем документооборота, так и отдельных хранящихся в них данных. Не останется в стороне и технология блокчейн, в рамках которой может быть реализована всесторонняя защита документов и документооборота, тем самым повышая эффективность работы организации. Интеграция научно-технического прогресса в конечном счёте одной из основных и наиболее приоритетных задач определяет в данной области полную стандартизацию СЭД, определяя позитивную динамику на рынке услуг в целом.

Ключевые слова: электронный документооборот, защита систем электронного документооборота, защита электронных документов, защита данных

MAIN DIRECTIONS OF DEVELOPMENT OF THE SECURITY ELECTRONIC DOCUMENT FLOW SYSTEMS IN THE MODERN TIMES

[1,2]Zhigalov K.Yu., [2]Podlevskikh A.P., [3]Avetisyan K.R.

[1]V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, e-mail: kshakalov@mail.ru;
[2]Moscow Technological Institute, Moscow, e-mail: kshakalov@mail.ru;
[3]Moscow University of the Ministry of Internal Affairs of the Russian Federation of V.Ya. Kikotya, Moscow, e-mail: Karen-Avetisyan-1989@bk.ru

For the time being, electronic document management is gaining popularity, it can be found not only in individual organizations, but also on various kinds of interactions between structures and organizations (e-government). The last aspect allows us to speak with confidence about the need to develop electronic document management security systems in modern conditions. The article focuses on the basics and principles of document management systems for small and medium-sized organizations. The tasks of protection of the electronic document management system and the requirements to the system put forward to ensure its security are listed. On the basis of a comprehensive analysis of existing systems and methods of protection developed the main directions of development of this kind of systems. The proposed directions of development of electronic document management security systems, with their simultaneous implementation, will improve the protection of both the document management systems and individual data stored in them. The blockchain technology will not stand aside, within the framework of which comprehensive protection of documents and document flow can be implemented, thereby increasing the efficiency of the organization. Integration of scientific and technological progress in the final analysis is one of the main and highest priorities in this area determines the full standardization of EDS, determining the positive dynamics in the service market as a whole.

Keywords: electronic document flow, electronic document flow systems protection, electronic documents protection, data security

В современных условиях резко возрастает количество контрагентов, как внутри, так и вне организации, в связи с чем увеличивается и документооборот между ними. Основные тенденции, связанные с оптимизацией делопроизводства, ориентированы на максимальную автоматизацию всех связанных с ними процессов и исключение бумажных носителей. Увеличение количества электронного документооборота, необходимого для принятия тех или иных автоматизированных управленческих решений или контрольных мероприятий, приводит к тому, что традиционные методы работы с документами становятся все более нерентабельными [1]. Кроме того,

автоматизированные системы не способны принимать какие-либо решения, базируясь на обработке документов на бумажных носителях. К тому же на перемещение документов на бумажных носителях, даже внутри компании, может тратиться до нескольких дней [2].

Учитывая, что перемещение и применение электронных документов связано с новыми для документооборота рисками киберпреступности, необходимо также принимать и факт ее наличия во внимание при разработке и внедрении автоматизированных СЭД.

Разновидность систем электронного документооборота

Потребность в эффективном управлении документами и привела к созданию автоматизированных систем электронного документооборота (СЭД) [2, 3]. Данные системы подразумевают создание электронных документов, их обработку, передачу, хранение и предоставление по запросу пользователю. В связи с хранением документов на электронных носителях особенно важным становится необходимость обеспечения сохранности данных [4, 5].

Считается, что каждая существующая система документооборота конкретно ориентирована в какой-либо области. Основными направлениями систем электронного документооборота являются [6, 7]:

– системы с ориентацией на хранение и поиск информации;

– системы со средствами «workflow». Они ориентированы на контроль маршрутизации документов;

– системы, ориентированные на оказание поддержки в принятии управленческих решений в организации, а также на накопление знаний. Эти системы являются «гибридными» и, как правило, объединяют в себе характеристики систем workflow и хранение информации;

– системы, ориентирующиеся на совместную работу или collaboration системы. Данные системы, в отличие от предыдущих, исключают понятие «иерархия организации»;

– системы с развитыми дополнительными сервисами. Например, это может быть сервис по управлению поставками, сервис по управлению колл-центра и т.д.

– комплексная система электронных документов (документационная система).

Такого рода система будет содержать в себе определенное количество программных подсистем и отвечать определенным требованиям.

Одними из важнейших задач, стоящими перед системами электронного документооборота, являются вопросы обеспечения целостности, доступности, резервирования и конфиденциальности информации [8]. Тем не менее в связи с относительно недавним получением такого рода системами широкого применения, вопросы защищенности данных, обрабатываемых в них, остаются открытыми.

На сегодняшний день в СЭД принято защищать не документы, а системы передачи, обработки и хранения электронных документов. В крупных компаниях такой подход реализован в виде доменных контроллеров, систем Firewall, систем шифрования данных и прочих традиционных для систем защиты данных решений.

При пересылке документов между организациями в настоящее время принято защищать документы электронными подписями с помощью криптографических систем. Электронные подписи, в настоящем их виде, несовершенны и вынуждают пользователей разбираться в особенностях их эксплуатации, что достаточно сложно даже для опытных пользователей. Дело в том, что каждая организация использует свои системы криптографических электронных подписей, что еще больше затрудняет вопрос ее применения. Кроме того, электронная подпись слабо защищает данные от изменений и не ведет их (изменений) какое-либо логирование.

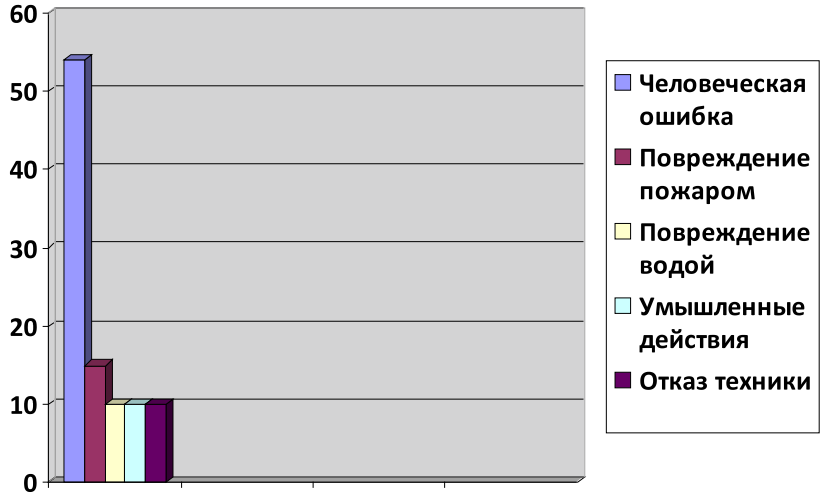
Основные опасности для информационных систем

Научно-исследовательским центром DataPro Research, Computer Security Institute, ФБР и компании Ernst&Young были проведены исследования (рисунок), согласно которым были выявлены основные причины повреждения и уничтожения информации.

Эти причины могут быть отнесены и к системам электронного документооборота: человеческая ошибка – 54%; повреждение пожаром – 15%; повреждение водой – 10%; умышленные действия – 10%; отказ техники – 10%.

К основным исполнителям действий отнести следующие категории: сотрудники компании – 81%; бывшие работники компании – 6%; посторонние люди – 13%.

Из статистики видно, что существующие подходы к обеспечению безопасности не оправданы и в реальности практически не защищают систему, хотя их стоимость достаточно высока, а сама система в результате достаточно громоздка, и связано это, в основном с необходимостью осуществления защиты в первую очередь от самих сотрудников этих компаний.



Причины повреждения у уничтожения документов

В связи с чем программные средства защиты информации целесообразно наиболее эффективно реализовать в виде дополнительных модулей системы документооборота в зависимости от условий их дальнейшего применения.

Это таит в себе определенные сложности для пользователя при налаживании электронного документооборота между организациями, так как каждая отдельно взятая компания использует надстройки своего производителя СЭД, при этом между собой они редко коррелируют [9].

Основные пути совершенствования уровня защищенности СЭД

Все означенные выше системы электронного документооборота имеют те или иные встроенные функции безопасности, которые в целом основаны на разграничении прав доступа в зависимости от роли, которую играет пользователь системы. Но это не сможет предотвратить угрозу несанкционированного использования конфиденциальной информации авторизованным пользователем. Поэтому большинство экспертов считают СЭД одним из элементов корпоративной информационной структуры, которая должна защищаться не отдельно, а в рамках единой политики обеспечения информационной безопасности организации, таким образом, защищенность электронного документооборота, прежде всего, определяется защищенностью инфраструктуры.

На сегодняшний день основная идея защищенного электронного документооборота состоит в том, что к задаче защиты системы электронного документооборота надо подходить с точки зрения классической защиты информационной системы. Следующим шагом все производители и разработчики СЭД будут использовать механизмы, обеспечивающие следующие функции [10]:

1) контроль целостности используемого программного обеспечения (в основном легко организуется за счет применения средств антивирусной защиты);

2) регистрацию событий в информационных системах (проведенные нами исследования показывают, что данную функцию возможно использовать с помощью механизма внедрения матрицы доступа с фиксацией не только факта доступа, но и характера изменений или же за счет технологий Blockchain);

3) криптографическую защиту (может быть организована различными методами от шифрования базы данных до шифрования физических носителей информации);

4) межсетевое экранирование (организовывается за счет стандартных на сегодняшний день средств системного и сетевого администрирования);

5) виртуальные частные сети (организуется за счет стандартных на сегодняшний день средств системного и сетевого администрирования);

6) аудит информационной безопасности.

Как говорилось ранее, большую часть перечисленных выше механизмов возможно достаточно легко реализовать в любой существующей системе документооборота в виде модулей либо отдельных программных продуктов (решений). Такого рода предложения не повлекут за собой существенных финансовых и трудовых затрат, в то время как результат для безопасности организации в целом будет достаточно ощутим. При написании статьи авторами было

опробовано тестовое внедрение дополнительных модулей в следующие системы электронного документооборота: 1С: Документооборот; DocsVision; IT-Inco; Optima-WorkFlow; RBC Docs; VisualDoc; Дело.

Что подчеркивает возможность применения модульности системы обеспечения безопасности электронного документооборота в практическом выражении.

Тем не менее, если обратить пристальное внимание на современные тенденции в информационных системах в целом, для электронного документооборота возможно использовать технологии из мира криптовалюты.

Проведенный анализ показывает, что обмен между контрагентами различного вида документами возможно осуществлять с помощью технологии Блокчейн (Blockchain). Данная технология представляет собой выстроенную по определенным правилам непрерывную последовательность цепочки блоков, содержащих информацию. Чаще всего данная цепь децентрализована, а информация в ней подтверждается следующими блоками. Особенность данной технологии в том, что цепь может содержать и распространять любую информацию во взаимосвязанных блоках.

Хотя в настоящее время данные технологии применяются в основном для криптовалют, уже существуют и разрабатываются другие проекты. Так, в 2014 г. была создана компания Bitnation которая начала предоставлять услуги по удостоверению личности, нотариату и т.д. А в 2016 г. Шведский земельный комитет начал тестирование данной технологии для переноса на ее основу базы данных земельных участков в Швеции. В 2018 г. Сбербанк РФ начал использование платформ на основе Блокчейн для анализа денежных потоков.

Исходя из проведенных авторами исследований применение системы Блокчейн для СЭД позволит максимально эффективно реализовать функции регистрации событий, проверки целостности, криптографической защите, подтверждению личности отправителя или подписанта и хранению документов. Что, в свою очередь, позволит практически полностью реализовать функции безопасного и достоверного документооборота как внутри организаций, так и между контрагентами.

В проведенном авторами исследовании возможности использования данной технологии в системе электронного документооборота было сделано следующее:

1. Перевод на платформу внутри корпоративного документооборота нескольких тестовых организаций. Единственная проблема, с технической точки зрения – это необходимость постоянного подключения к сети Интернет и некоторое время на проведение транзакций и подтверждений по сети.

2. В качестве тестовой платформы была использована сеть Spread – она отвечала параметрам скорости транзакций, достаточной дешевизны ее обслуживания в виде размещения собственных вычислительных мощностей на ее базе.

Описанное выше решение позволило отказаться от СУБД в привычном нам виде при использовании электронного документооборота внутри компании. На данный момент движение всех документов можно легко отследить по цепочке.

Возможно, что повсеместное применение систем на основе технологии Блокчейн столкнется с вопросами юридического характера, так как на сегодняшний момент нет ни одного правоустанавливающего акта на данную тему, но это лишь вопрос времени, так как на данные технологии уже обратили на себя внимание банковские структуры, для проводки финансовых транзакций, в рамках информационных систем которых вирируется в том числе информация, относящаяся к категории персональных данных, что побудит их (банки) всерьез заняться вопросами юридической подоплеки. Тем не менее этот факт не должен мешать развитию технологии на этапах внедрения документооборота внутри компаний [11].

С точки зрения безопасности технологии Блокчейн, существует вероятность подмены целой цепочки со стороны киберпреступников, но для этого необходимо очень большое количество вычислительных мощностей. Следует отметить, что с начала использования технологий Блокчейн и Биткоин официально не зафиксировано ни одного взлома цепи.

Выводы

Документооборот материализует процессы сбора, преобразования, хранения информации, а также процессы управления: подготовку и принятие решений, контроль за их выполнением. Защита информации в системах документооборота – насущная необходимость современного функционирования любого предприятия. Построение оптимальных систем с точки зрения их защищенности предполагает учет большого числа параметров, которые необходимо оценить. Учитывая сложность формализации параметров информационных объектов, влияние на процесс множества факторов, изменяющихся, а также сложность определения их количественных показателей, ре-

шение поставленных задач требует применения аппарата теории нечетких множеств и сложной системы экспертных оценок.

Хотя выбор конкретных средств защиты зависит от ценности информации, типа СЭД и конкретной организации, в настоящее время имеет смысл обратиться к статистике и строить систему, ориентированную именно на нее. Тем не менее в любом случае, опираясь на статистику исследований DataPro Research, Computer Security Institute, ФБР и компании Ernst&Young описанную выше, должны быть внедрены элементарные, самые дешевые и от этого не менее эффективные средства – вход в систему документооборота должен осуществляться по системе паролей с разграниченным уровнем доступа. Физический доступ в помещение, где установлена система управления документооборотом, должен осуществляться по правилам внутреннего распорядка и быть ограниченным для посторонних лиц [12].

Основная проблема развития систем защиты электронного документооборота в их разрозненности, большой номенклатуре систем криптографической защиты, что существенно затрудняет работу конечного пользователя на всех этапах работы с документами.

В среднесрочной перспективе наиболее эффективно применение технологий Блокчейн для осуществления всесторонней защиты документов. Технология позволит осуществлять эффективную защиту предприятиям любого размера без особых трудозатрат, а значит, повысит эффективность их работы. Кроме того, повсеместное применение технологии позволит наконец полностью стандартизовать СЭД и протоколы, что положительно скажется на рынке в целом.

Список литературы

1. Досмухамедов Б.Р. Анализ угроз информации систем электронного документооборота // Компьютерное обеспечение и вычислительная техника. 2009. № 6. С. 140–143.

2. Загальне Діловодство // studbooks.net [Электронный ресурс]. URL: http://studbooks.net/60524/dokumentovedenie/obschee_deloproizvodstvo_ (дата обращения: 10.11.2018).

3. Жигалов К.Ю. Использование современных методов получения и обработки информации для целей создания геоподоснов ГИС-систем // Естественные и технические науки. 2012. № 4 (60). С. 209–212.

4. Маркова С.В. Безопасность электронного документооборота // Прикладные исследования и технологии ART2015 Сборник трудов международной конференции. 2015. С. 185–189.

5. Маркова С.В. Особенности обеспечения безопасности данных в современных СУБД // Технологии информационной безопасности в деятельности органов внутренних дел. 2016. С. 135–142.

6. Петухов С.Г., Жигалов К.Ю. Современные тенденции обеспечения защиты информации в малом и среднем бизнесе России // Прикладные исследования и технологии ART2016. Сборник трудов международной конференции. 2016. С. 251–256.

7. Построения и функционирования систем управления документами (СУД) // Market Journal [Электронный ресурс]. URL: http://www.market-journal.com/itvupravlenii/19.html (дата обращения: 18.11.2018).

8. Путькина Л.В. Роль информационных систем и технологий в управлении предприятиями сферы услуг // Nauka-rastudent.ru. 2016. № 05 (029) [Электронный ресурс]. URL: http://nauka-rastudent.ru/29/3463/ (дата обращения: 01.11.2018).

9. Путькина Л.В. Особенности использования электронного документооборота для эффективной работы современного предприятия // Nauka-rastudent.ru. 2016. № 01 (25) / [Электронный ресурс]. URL: http://nauka-rastudent.ru/25/3173/ (дата обращения: 01.11.2018).

10. Сабанов А.А. Некоторые аспекты защиты электронного документооборота // Connect! Мир связи. 2010. № 7. С. 62–64.

11. Маркова С.В. Актуальные проблемы по защите персональных данных и методы их решения // Прикладные исследования и технологии ART2016. Сборник трудов международной конференции. 2016. С. 183–186.

12. Подлевских А.П., Норец В.А. Обеспечение информационной безопасности от несанкционированного проникновения в сетях // Образовательная среда сегодня и завтра: материалы VIII Международной научно-практической конференции. Под общ. ред. Г.Г. Бубнова, Е.В. Плужника, В.И. Солдаткина. 2014. С. 325–328.