УДК 004.056

Т.И. Булдакова, Б.В. Глазунов, Н.С. Ляпина

Оценка эффективности защиты систем электронного документооборота

Рассмотрены особенности применения систем электронного документооборота, дан обзор угроз и подходов к обеспечению безопасности. Поставлена задача защиты электронного документооборота. Осуществлен выбор показателя оценки эффективности и анализ возможных способов его расчета.

Ключевые слова: системы электронного документооборота, информационная безопасность, критерии эффективности.

Управление электронными документами. Электронный архив и хранилище данных

Эффективность управления организацией во многом зависит от решения задач оперативного и качественного формирования электронных документов, контроля их исполнения, а также продуманной организации их хранения, поиска и использования. Потребность в эффективном управлении электронными документами привела к созданию систем электронного документооборота (СЭД), под которыми понимают организационно-технические системы, облегчающие процесс создания, управления доступом и распространения электронных документов в компьютерных сетях, а также обеспечивающие контроль над потоками документов в организации. По данным ряда аналитиков, производительность труда персонала при использовании СЭД увеличивается на 20–25%, а стоимость архивного хранения электронных документов на 80% ниже по сравнению со стоимостью хранения бумажных архивов [1].

Применение систем электронного документооборота позволяет сотрудникам контролировать прохождение документов и доступ к ним, управлять хранением и публикациями документов, минимизировать избыточность данных и бумажные процессы. Поэтому с помощью СЭД повышается эффективность деятельности коммерческих компаний и промышленных предприятий, а в государственных учреждениях на базе технологий электронного документооборота решаются задачи внутреннего управления, межведомственного взаимодействия и взаимодействия с населением, что является необходимым условием для перехода к «электронному» правительству. В настоящее время практически все федеральные органы государственной власти используют СЭД для ведения централизованного учета и регистрации входящих и исходящих документов, их перевода и хранения в электронном виде, а также учета результатов их исполнения.

В последнее время развитие СЭД направлено в основном на совершенствование сервисных возможностей, так как базовые возможности в той или иной форме уже реализованы. Кроме того, можно отметить развитие СЭД в сторону управления различного вида контентом (мультимедиа), использование технологий автопроцессинга и разбора содержания документа.

Ряд существующих СЭД позволяет вести электронные архивы, наполнение которых происходит через системы потокового сканирования и ввода бумажных документов, автоматизированной обработки электронной почты, а также запросов и обращений, поступающих через ведомственные интернет-сайты. Используемые системы обеспечивают прохождение этих документов до структурного подразделения или подведомственной организации, учет и контроль своевременности их рассмотрения и исполнения. Наличие электронного архива создает основу для управления, доступа и интеграции важной деловой информации. С его помощью можно объединить все формы данных – документы, Web, изображения и аудиовизуальную информацию – в различных рабочих процессах и приложениях. Участники процесса получают возможность составлять, заполнять, просматривать, редактировать, визировать и публиковать документы в электронной форме с высокой степенью безопасности и с использованием Интернета или Интранета. Таким образом, электронный архив предназначен для перевода бумажных документов в цифровую форму и управления всеми видами электронных документов и аудиовидеоматериалов. Он позволяет:

– обеспечить высокую доступность и безопасность информации;

– поддерживать работу ключевых систем организаций;

– существенно сократить расходы на хранение и управление цифровой информацией;

– снизить убытки из-за потерь важных документов.

При всех преимуществах внедрение СЭД порождает новые риски, и пренебрежение защитой приводит к новым информационным угрозам.

Анализ угроз информационной безопасности в СЭД

Считается, что для защиты СЭД достаточно использования электронно-цифровой подписи (ЭЦП), однако в большинстве случаев разработчики не поясняют, как правильно использовать ЭЦП, какая нужна инфраструктура и какие защищенные сервисы необходимо развернуть на ее основе. Обычно на соответствующих сайтах приводятся только конкретные примеры реализованных защищенных СЭД. Поэтому понятие защищенного электронного документооборота (ЗЭД) определить достаточно трудно, особенно в условиях постоянно меняющегося правового поля, недостатка стандартов и активно развивающихся технологий.

В общем случае к задаче создания ЗЭД необходимо подходить с точки зрения классической защиты информационной системы [2], обеспечивая решение таких задач, как:

– аутентификация пользователей и разделение доступа;

– подтверждение авторства электронного документа;

– контроль целостности электронного документа;

– конфиденциальность электронного документа;

– обеспечение юридической значимости электронного документа.

Если раньше обеспечивалась защита непосредственно самих электронных документов или информационных ресурсов, содержащих документы, то теперь изменяются основной вектор атак и, соответственно, объект защиты [3]. Кроме традиционных атак на информационные ресурсы все чаще их объектом становится взаимодействие «человек – электронный документ», «человек – информационный ресурс». Таким образом, защищать надо не столько сами документы, сколько системы передачи, обработки и хранения электронных документов при доступе пользователей к работе с электронными документами.

Рассмотрим общую модель защищенной СЭД [4] и на ее примере проведем анализ существующих угроз информационной безопасности (рис. 1).

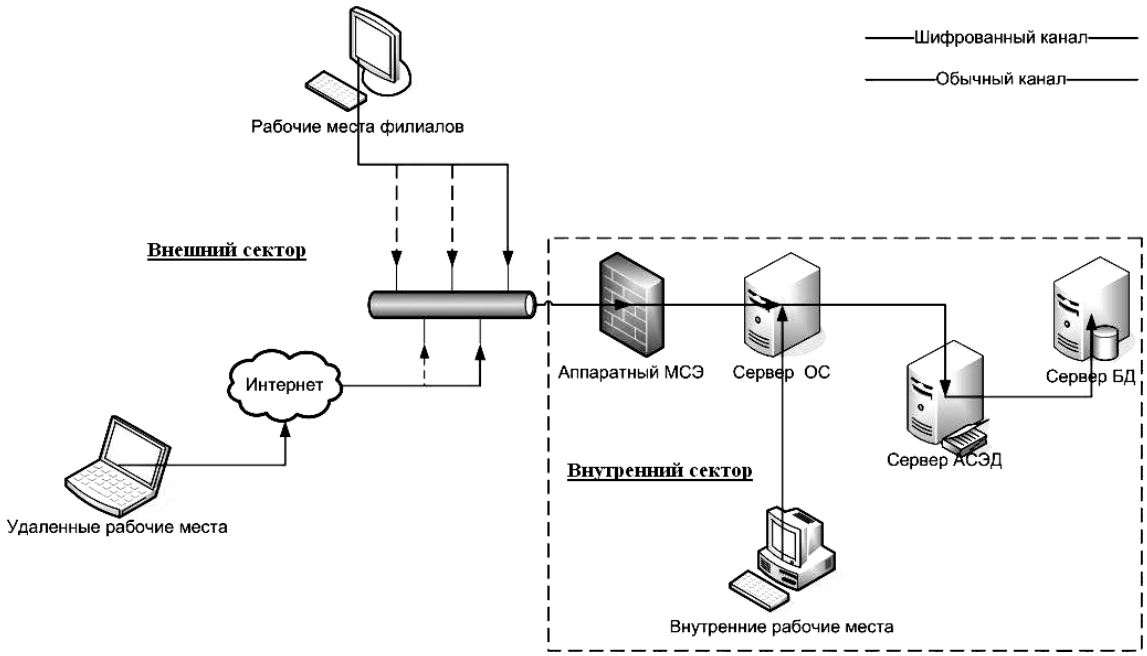

Рис. 1. Общая модель защищенной СЭД

Во внешний сектор входят удаленные рабочие места и рабочие места филиалов, которые основаны на локально-вычислительных сетях, защищенной Wi-Fi-сети, VPN-каналах и т.д. Во внутренний сектор входят аппаратный межсетевой экран (МСЭ) и сервер операционной системы (ОС) с поддержкой домена, который может быть организован на следующих платформах: Windows Server,

FreeBSD, Linux, Solaris. Сервер автоматизированной системы электронного документооборота (АСЭД) (сервер приложения) может иметь две реализации: прикладная программа для ОС и Web-интерфейс. Сервер базы данных (БД) реализован на основе клиент-серверных СУБД, к которым относятся MS SQL Server и Oracle. Все эти компоненты составляют единый механизм доступа к электронным документам. Во внутренний сектор входят также внутренние рабочие места, которые имеют прямой доступ к серверу ОС, в обход межсетевого экрана. Шифрованный канал представляет собой передачу данных по протоколу HTTPS, поддерживающему шифрование. Сервер ОС является одновременно и центром сертификации защищенного протокола.

Угрозы СЭД можно сгруппировать по нарушаемым свойствам безопасности: угроза конфиденциальности; угроза целостности; угроза доступности. Под угрозой конфиденциальности понимают такие нарушения, как кража, перехват информации, изменения маршрутов следования. Угрозы целостности – это угрозы, при реализации которых информация теряет заранее определенные системой вид и качество. Объектами данной угрозы могут быть все компоненты описанной выше модели СЭД: документы – данные, хранящиеся на сервере БД, резервные копии документов; сервер БД – среда хранения электронных документов; серверы ОС и АСЭД – установленные на серверах и рабочих станциях, включая клиентов СУБД, операционная система и интерфейсная часть СЭД; аппаратная система – каналы связи между компонентами, аппаратный межсетевой экран. Угрозы доступности характеризуют возможность доступа к хранимой и обрабатываемой в СЭД информации в любой момент времени. Защиту от этих угроз в той или иной мере должна реализовывать любая система электронного документооборота. При этом, с одной стороны, при внедрении СЭД увеличиваются риски реализации угроз, но, с другой стороны, при правильном подходе упорядочение документооборота позволяет выстроить более качественную систему защиты.

Таким образом, любая защищенная СЭД должна предусматривать реализацию как минимум следующих механизмов защиты: обеспечение целостности документов; обеспечение безопасного доступа; обеспечение конфиденциальности документов; обеспечение подлинности документов; протоколирование действий пользователей.

Постановка задачи защиты электронного документооборота

Задачу оценки эффективности защиты СЭД можно представить как задачу выбора таких имеющихся средств защиты, которые позволяют получить наиболее рациональную структуру и в ее рамках сформировать оптимальный состав средств, обеспечивающих перекрытие всех выявленных угроз безопасности с требуемой эффективностью. Постоянно меняющийся перечень угроз и отсутствие единого подхода к оценке эффективности системы защиты информации (СЗИ) делает рассматриваемую задачу необходимой и актуальной. Существуют качественные и количественные методы анализа эффективности СЗИ. Во многих случаях качественных оценок оказывается недостаточно, кроме того, количественные методы более точны. Однако для «измерения» эффективности необходимо иметь обоснованный критерий (показатель оценки эффективности системы). На практике встречаются следующие типы критериев:

– критерии типа «эффект – затраты», позволяющие оценивать достижение целей функционирования СЗИ при заданных затратах (так называемая экономическая эффективность);

– критерии, позволяющие оценить качество СЗИ по определенным показателям и исключить те варианты, которые не удовлетворяют заданным ограничениям. При этом используются методы многокритериальной оптимизации, восстановления функций и функционалов, методы дискретного программирования;

– искусственно сконструированные критерии, позволяющие оценивать интегральный эффект (например, «линейная свертка» частных показателей, методы теории нечетких множеств).

Следует учитывать, что СЗИ в целом является сложным объектом, выполняющим множество функций. Для каждого структурного элемента СЗИ и выполняемой функции возможно применение различных программных и технических средств, во множестве представленных на рынке [5]. Следовательно, в конкретном случае можно построить множество вариантов СЗИ, отличающихся структурой, составом, технико-экономическими показателями (быстродействие, надежность, стоимость и т.д.). Поскольку подобные показатели нередко бывают взаимно противоречивы, то выбор конкретного комплекса средств защиты информации (КСЗИ) приводит к необходимости решать оптимизационную задачу, требующую наличия показателей эффективности ЗИ и соответствующих критериев построения защиты.

Применительно к рассматриваемой задаче выбора средств защиты информации будем использовать следующий критерий: средства защиты информации должны удовлетворять максимальному количеству требований по защите информации и при этом обеспечивать минимальную стоимость. Поэтому рассмотрим оптимизационный (комбинаторный) подход.

Пусть имеется $M = \{1, \ldots, m\}$ – множество требований по защите информации; $N = \{1, \ldots, n\}$ – множество средств защиты, реализующих различные способы и функции защиты и возможных для применения в конкретном случае; $c_1, \ldots, c_n$ – цены на средства защиты информации. Требуется определить необходимый набор средств защиты информации $x_1, \ldots, x_n$, чтобы стоимость решения была минимальной, а выбранные средства обеспечивали закрытие требований по защите информации. Таким образом, необходимо решить следующую задачу оптимизации:

$$\sum_{j=1}^{n} c_j x_j \to \min$$

при выполнении заданных ограничений

$$\sum_{j=1}^{n} a_{ij} x_j \geq 1, \ \ i = 1,\ldots,m;$$

$$x_j \in \{0;1\}, \ j = 1,\ldots,n;$$

$$a_{ij} = \begin{cases} 1, & \text{если } j\text{-е средство закрывает } i\text{-е требование,} \\ 0, & \text{в противном случае,} \end{cases}$$

где a_{ij} – коэффициенты покрытия.

Таким образом, получим задачу о покрытии множества, которая является задачей целочисленного линейного программирования. Рассмотрим возможные методы решения поставленной задачи.

Выбор и обоснование метода решения задачи

Для решения задач целочисленного линейного программирования используется ряд методов:

– методы отсечения, базирующиеся на использовании процедуры линейного программирования для последовательности задач, в которую по мере решения вводятся особые дополнительные ограничения;

– комбинаторные методы, в которых вместо процедуры линейного программирования используют сокращение поиска возможных решений с помощью анализа исходного множества решений;

– приближенные методы, применяющиеся для решения задач большой размерности, которое в значительной степени затруднено дефицитом временных и технических ресурсов;

– человеко-машинные методы, требующие значительных вычислений.

Так как использование большого числа средств защиты информации ($n \geq 20$) не представляется целесообразным, а также из-за требований к быстродействию алгоритма, рассматривать приближенные и человеко-машинные методы не будем. Также отметим, что в отличие от методов отсечений метод ветвей и границ значительно меньше подвержен влиянию ошибок округления. Поэтому в качестве алгоритма решения поставленной математической задачи предлагается использовать его.

Суть метода ветвей и границ заключается в упорядоченном переборе вариантов и рассмотрении лишь тех из них, которые оказываются по определенным признакам перспективными, и отбрасывании бесперспективных вариантов. С этой целью множество допустимых решений (планов) некоторым способом разбивается на подмножества, каждое из которых этим же способом снова разбивается на подмножества. Процесс продолжается до тех пор, пока не будет получено оптимальное целочисленное решение исходной задачи [6].

Организация защищенного документооборота

Разработка СЗИ СЭД должна проводиться с учетом защиты от выявленных угроз и возможных информационных рисков, для которых определяются способы защиты, и на основе предложенного показателя оценки ее эффективности. При этом учитываются требования, которые предъявляются к созданию таких систем, а именно [7]:

– организация защиты информации осуществляется с учетом системного подхода, обеспечивающего оптимальное сочетание взаимосвязанных методологических, организационных, программных, аппаратных и иных средств;

– система должна развиваться непрерывно, так как способы реализации угроз информации непрерывно совершенствуются. Управление ИБ – это непрерывный процесс, заключающийся в обос-

новании и реализации наиболее рациональных методов, способов и путей совершенствования систем ИБ, непрерывном контроле, выявление ее «узких» и слабых мест, потенциальных каналов утечки информации и новых способов несанкционированного доступа (НСД);

– система должна предусматривать разделение и минимизацию полномочий по доступу к обрабатываемой информации и процедурам обработки;

– система должна обеспечивать контроль и регистрацию попыток НСД, содержать средства для точного установления идентичности каждого пользователя и производить протоколирование действий;

– обеспечивать надежность защиты информации и контроль за функционированием системы защиты, т.е. использовать средства и методы контроля работоспособности механизмов защиты.

Реализация перечисленных требований при создании системы защиты информации в СЭД будет способствовать организации эффективного защищенного документооборота.

Литература

1. Макарова Н.В. Компьютерное делопроизводство: учеб. курс / Н.В. Макарова, Г.С. Николайчук, Ю.Ф. Титова. – СПб.: Питер, 2005. – 411 с.

2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – М.: ДиаСофт, 2002. – 693 с.

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

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

5. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – М.: Наука и техника, 2003. – 384 с.

6. Зайченко Ю.П. Исследование операций: учеб. – 6-е изд., перераб. и доп. – Киев: Изд. дом «Слово», 2003. – 688 с.

7. Аскеров Т.М. Защита информации и информационная безопасность / под общ. ред. К.И. Курбакова. – М.: Российская экономическая академия, 2001. – 386 с.

Булдакова Татьяна Ивановна
Д-р техн. наук, проф. каф. информационной безопасности МГТУ им. Н.Э. Баумана
Тел.: 8 (499) 263-69-36
Эл. почта: buldakova@bmstu.ru

Глазунов Борис Викторович
Студент каф. информационной безопасности МГТУ им. Н.Э. Баумана
Тел.: 8 (499) 263-69-36
Эл. почта: restable@gmail.com

Ляпина Наталья Сергеевна
Магистрант каф. информационной безопасности МГТУ им. Н.Э. Баумана
Тел.: 8 (499) 263-69-36
Эл. почта: lyapinans@gmail.com

Buldakova T.I., Glazunov B.V., Lyapina N.S.

Assessment of efficiency of protection of systems of electronic flow of documents

Features of systems of electronic flow of documents are considered, the overview of threats and approaches to safety is given. The problem of the protection of electronic documents is formulated. The choice of an indicator of an assessment of efficiency is made, and the analysis of possible ways of its calculation is carried out.
Keywords: systems of electronic flow of documents, information security, criteria of efficiency.