Электронные архивы: методологический подход к решению проблемы катастрофоустойчивости при долговременном хранении

Г. П. Акимова, М. А. Пашкин, Е. В. Пашкина, А. В. Соловьев, Д. В. Соловьев

Аннотация. Статья является продолжением серии статей, посвященных проблемам проектирования, создания и внедрения электронных архивов. В статье изложены суть проблемы устойчивости к воздействиям катастрофического характера и методологический подход к решению данных проблем при долгосрочном хранении электронных документов в системах электронного архива (ЭА). Представленная работа является обобщением опыта создания электронных архивных систем долговременного хранения.

Ключевые слова: э*лектронный документооборот, катастрофоустойчивость, электронный архив, система управления электронными документами, электронный документ, автоматизация архивного дела.*

Введение

Как было показано в предыдущих статьях ([1, 19]), при длительном хранении необходимо принимать дополнительные технические меры для решения проблем сохранности, аутентичности и интерпретируемости данных и носителей информации в ЭА. При этом информационная избыточность ЭА возрастает пропорционально важности документов и величине сроков хранения. Кроме того, при длительном хранении ценных документов необходимо продумывать решения, позволяющие не только обеспечить безопасность хранения, в смысле защиты от несанкционированного доступа, надежность хранения, в смысле обеспечения бесперебойности работы программных и технических средств ЭА, но и обеспечить сохранность данных при возможном воздействии катастрофического характера. Под таким воздействием понимается необходимость обеспечения сохранности данных при природных, техногенных или иных воздействиях, приводящих к массовому выходу из строя программно-технических средств (ПТС) ЭА, невозможности использовать запасное имущество и принадлежности (ЗИП), формирующих риск полной потери информации.

В предлагаемой статье обобщены рекомендации по созданию математического и методологического аппарата количественной оценки катастрофоустойчивости ЭА, приведены рекомендации по повышению уровня защиты защите данных ЭА от катастрофического воздействия. Выделены проблемы и возможные пути их решения, которые могут помочь разработчикам электронных архивов в будущем.

1. Основные понятия и определения

Электронный архив (ЭА) — структурированное хранилище неизменяемых электронных оригиналов документов (электронных изображений бумажных документов), созданное на основе законов и правил ведения архивов на конкретной территории (в конкретной стране).

Длительное хранение — хранение электронных документов сроком от 5 лет и до «сотен лет» (фактически бессрочно) (см. [19]).

Долговременная сохранность — период времени, в течение которого электронные документы поддерживаются в качестве доступного и аутентичного свидетельства (доказательства) [2].

Аутентичный электронный документ — электронный документ, точность, надежность и целостность которого сохраняются с течением времени [2].

Катастрофоустойчивость — способность к восстановлению работы приложений и данных ЭА за минимально короткий период времени после катастрофы.

Под катастрофами (воздействиями катастрофического характера) подразумеваются не только пожар, наводнение, землетрясение, но и возможные непредвиденные сбои в работе служб, разрушение данных или повреждение центров обработки данных (ЦОД), например, в случае разрыва телекоммуникационных линий, возникших в результате проведения ремонтных работ, умышленной диверсии, саботажа, по халатности или вследствие ошибочных действий обслуживающего персонала.

2. Проблемы обеспечение катастрофоустойчивости ЭА

Огромный объём обрабатываемой и хранящейся информации в ЭА длительного хранения, сложность выполняемых функций, а также ценность хранящихся электронных документов и данных, определяют необходимость создания механизмов, позволяющих оперативно прогнозировать и вычислять вероятность отказов и катастроф при воздействии различных дестабилизирующих факторов, а также выбирать стандартные меры противодействия, разрабатывать алгоритмы функционирования систем с учетом возможных воздействий катастрофического характера.

В обычном «бумажном» архиве также применяются меры, способные противодействовать катастрофам (противопожарные, охранные и т. д.). В каком-то смысле бумажный документ сложнее уничтожить «бесследно» в отличие от электронного, документы которого можно просто «удалить из системы». Однако у электронного документа есть то преимущество, что он может храниться в нескольких местах в нескольких копиях, что может обеспечить сложность его уничтожения полностью. Кроме того, электронный документ может быть защищен сложной системой связей, прав доступа, протоколов действий пользователей и т. д., затрудняющих уничтожение.

В предыдущих статьях мы говорили, что при долговременном хранении неизбежно присутствует избыточность данных для снижения рисков не интерпретируемости (не читаемости), нарушения аутентичности, ненадежности хранения. Обеспечение катастрофоустойчивости также добавит избыточности при хранении данных в ЭА.

Однако, вся проблема заключается в том, что достаточно сложно продумать разумную избыточность при длительном хранении данных, так как необходимо уметь оценивать риски катастроф, своевременно выявлять изменение рисков и, тем самым, корректировать модели угроз, а также проводить оценку рисков в течение срока хранения документов в ЭА, обеспечивать выбор и проведение контрмер.

Без постоянного контроля уровня защищенности от катастроф ЭА, прогноза рисков и упреждающей разработки контрмер избыточность хранения может превратиться в расточительность при поддержании работоспособности и без того дорогого решения ЭА длительного хранения.

3. Возможные пути решения проблем катастрофоустойчивости ЭА

Итак, мы определили катастрофоустойчивость как способность к восстановлению работы приложений и данных ЭА за минимально короткий период времени после катастрофы. В отличие от отказоустойчивых систем, которые должны продолжать функционирование в случае сбоя одного или нескольких компонентов, катастрофоустойчивый ЭА должен сохранять работоспособность в случае одновременного множественного выхода из строя составных частей в результате внезапных воздействий.

Вследствие этого построение прогноза поведения ЭА в условиях катастрофических воздействий требует создания полноценной модели функционирования ЭА под влиянием различных дестабилизирующих факторов, а также моделирования мер противодействия данным факторам. Процесс создания такой модели будем называть моделированием катастрофоустойчивости ЭА.

Ниже предложены концепция и общий методологический подход к созданию моделей поведения ЭА в условиях катастрофических воздействий, а также оговорены основные принципы и допустимые ограничения при построении таких моделей.

3.1. Основные положения концепции катастрофоустойчивости ЭА

Основные положения концепции катастрофоустойчивости ЭА тесно связаны с общим методологическим подходом, на котором основано проектирование ЭА. Создание и моделирование мер противодействия катастрофам должно идти вместе с проектированием ЭА. Ниже под элементами ЭА будем понимать центры обработки данных (ЦОД), состоящие из ПТС различных уровней и назначения, а также оборудование и каналы связи (ОКС) различных уровней; под узлами ЭА будем понимать конкретное оборудование, входящее в ЦОД и ОКС. Характеристики ПТС, ОКС, ЦОД, описание воздействия катастрофического характера должны храниться в отдельной БД, являющейся основой для моделирования катастроф и мер противодействия им.

В основе концепции лежит моделирование основного технологического цикла работы ЭА при

воздействии на систему дестабилизирующих факторов [11–14].

1. При моделировании работы временные характеристики движения информационных потоков в модели ЭА должны задаваться из учета характеристик ее элементов (описание узлов ЦОД, ОКС, их технические характеристики, принцип действия и особенности должны храниться в отдельной БД) и квалификации обслуживающего персонала ЭА [9].

Движение информационных потоков должно моделироваться с учетом влияния на ЭА различных ДФ (отказы электропитания, изменение климата внутри помещений ЦОД, пожарная опасность, отказы элементов ЦОД, модели умышленного ущерба и влияния человеческого фактора [3, 6–9]). Характеристики ДФ, а также сценарии развития катастрофических ситуаций, должны задаваться отдельными параметрическими моделями и храниться в отдельной БД.

Результатом моделирования должно быть вычисление показателей катастрофоустойчивости, надежности [4] и эффективности работы [5] ЭА, а также качественные выводы о готовности ЭА к выполнению своих функций при развитии заданных катастрофических событий с анализом причин нарушения устойчивости системы на основе полученной информации.

В отдельной БД должна накапливаться и храниться «история» развития реальных проблем, возникавших при эксплуатации системы, для построения модели ретроспективного анализа развития катастрофических событий и оценки эффективности контрмер [17].

2. При моделировании катастрофоустойчивости должен применяться сценарный метод («что, если») анализа и прогнозирования поведения ЭА с учетом влияния дестабилизирующих факторов (ДФ) [13, 14, 16].

Моделирование поведения ЭА должно производиться, исходя из предположения, что катастрофическое событие состоялось. Необходимо смоделировать состояние, движение информационных потоков, влияние отказа элемента на поведение ЭА с учетом времени восстановления элемента.

Сценарий развития катастрофических событий, степень влияния воздействия ДФ на ЭА должны задаваться отдельными параметрическими моделями, в которых параметрами выступают степень воздействия, вероятность возникновения, наличие средств противодействия ДФ.

Вероятность возникновения катастрофы (наводнения, например) оценить крайне трудно, а иногда и бессмысленно, так как вероятность может быть сколь угодно малой. Вместо этого должны проводиться оценки вероятности выполнения мер по восстановлению работоспособности ЭА после того, как произошло предполагаемое катастрофическое воздействие на систему.

3. При оценке состояния и степени готовности ЭА к выполнению своих функций должно применяться ретроспективное моделирование поведения системы (на основе анализа БД «истории» (ретроспективы) отказов, принципа работы различных конфигураций ЭА, ранжированных по степени важности рисков возникновения катастрофы, моделей ДФ).

Моделирование отказов элементов ЭА должно производиться не только с учетом «истории» катастроф, но и также по случайному закону распределения отказов в ее элементах, как это делается при обычной оценке надежности системы [4].

При оценке состояния ЭА, а также оценке риска возникновения аварийной или критической ситуации должен использоваться анализ «истории» отказов ее элементов и вариантов разрешения проблем (восстановления) с оценкой эффективности контрмер.

Хранение «истории отказов» также вносит существенную избыточность в ЭА, однако это единственный способ «вспомнить», что происходило с системой много лет назад, особенно в условиях, когда обслуживающий персонал ЭА за это время поменялся.

4. Модель катастрофоустойчивости ЭА должна быть расширяемой и предусматривать:

– ввод новых моделей ДФ, их характеристик и функций воздействия на ЭА;
– обработку новых статистических данных по «истории» отказов и изменению конфигурации ЦОД, ОКС, отдельных ПТС.

5. Модель катастрофоустойчивости ЭА должна обладать свойством непротиворечивости, т. е. должна соблюдаться непротиворечивость принципам функционирования ЭА.

3.2. Ограничения и допущения модели оценки катастрофоустойчивости ЭА

При проектировании модели катастрофоустойчивости ЭА могут быть приняты следующие допущения:

1) все последствия катастрофических воздействий на ЭА по причинению ущерба адекватны первопричине (например, пожар, вызванный землетрясением или ураганом и т. п.), поэтому при моде-

лировании катастрофоустойчивости принимается во внимание только первопричина;

2) система обеспечения катастрофоустойчивости ЭА проектируется таким образом, что резервные объекты (если таковые имеются), которым переданы функции ЦОД или иных элементов ЭА, попавших под воздействие катастрофы, выполнят поставленную перед ними задачу;
3) риски возникновения и развития катастроф могут быть по последствиям оценены так, что передача функций резервным объектам обязательна, независимо от того, что ущерб от катастроф может быть меньше, чем спрогнозирован;
4) восстановление функционирования элементов ЭА с заданным уровнем доверительной вероятности (обеспечение достоверности, полноты и своевременности выполнения функций ЭА) проводится за время, не превышающее заданное.

3.3. Методологический подход к оценке катастрофоустойчивости ЭА

В качестве методологи количественной оценки катастрофоустойчивости ЭА может быть принята следующая методология, разработанная авторами статьи и прошедшая проверку практикой. Ниже предложена последовательность шагов методологии и математические модели, которые могут быть взяты за основу для составления методики оценки катастрофоустойчивости при проектировании и создании конкретного ЭА.

1. Как было сказано выше, в основу методологического подхода моделирования катастрофоустойчивости ЭА закладывается сценарный подход. То есть предположение, что воздействие катастрофического характера произошло, необходимо оценить влияние его на функционирование системы и определить достаточность контрмер (в том числе средств резервирования) для компенсирования влияния ДФ, а также действия для восстановления работоспособности ЭА в полном объеме [13, 14].

Ограничениями при этом могут выступать ценность электронных документов (в том числе нематериальная), показатели надежности, эффективности, потенциальной пожарной опасности, доступности информационных ресурсов, устойчивости связи, энергетической безопасности (например, бессбойное электроснабжение) и др. конкретного элемента системы. Числовые значения показателей, определяющие потенциально уязвимые элементы ЭА, должны быть получены на основе исследований или статистического анализа функционирования ЭА и сохранены в отдельной БД. Должна быть предоставлена возможность изменения БД при изменении состава ПТС ЭА, переконфигурирования ПТС ЭА и т. д.

2. Определяется важность элементов ЭА.

Коэффициент важности каждого элемента ЭА системы определяется в зависимости от выполняемых элементом функций, ценности информации, потенциальной уязвимости и т. д. Например, учитывая типы ЦОД и ОКС, можно ввести обозначения: пусть b_1 соотносится с головным ЦОД, b_{2j} — с j-м региональным ЦОД, b_{3k} — с k-м районным ЦОД и т. д. Таким образом, в общем случае получаем следующее соотношение: $1 \geq b_1 > b_{2j} > b_{3k}$. (1)

Назначение приоритетов даёт основание считать, что различен ущерб, нанесённый для элементов различных приоритетов в результате действия одной и той же катастрофы.

3. Модели ДФ функционирования ЭА.

Должен быть определен состав ДФ, влияющих на работу ЭА, произведено их ранжирование по степени нанесения ущерба.

Все ДФ разделяются на те, на которые обслуживающий персонал ЭА, сервисные центры и др. могут повлиять, и те, на которые никто повлиять не может (ураган, цунами, землетрясение и т. д.).

Для ДФ, на которые можно повлиять в сторону их уменьшения, составляются модели их влияния на систему: создается модель ДФ, модели воздействия на ЭА и модели компенсации или предотвращения последствий. Для всех ДФ необходимо установить, что является объектом воздействия в каждом конкретном случае (ЦОД, ОКС в целом или их отдельный узел: сервер, канал связи и т. д.).

Для оценки ДФ определяются необходимые статистические данные и порядок их сбора (обследование, анкетирование, как один из методов экспертной оценки, получение данных от сервисных центров, подсистем контроля функционирования ЭА и т. д.). Затем производится сбор необходимых статистических данных для количественной оценки или, в случае невозможности, качественной оценки степени влияния ДФ.

По определенным ниже частным показателям производится оценка влияния ДФ. Таким образом, может определяться математическая модель количественной оценки влияния ДФ на элементы и узлы ЭА.

Для ДФ, оценка влияния которых на ЭА определяется только качественно, могут вводиться 3 величины: минимальная вероятность возникновения («оптимистический» прогноз), максимальная вероятность («пессимистический» прогноз), наибольшая вероятность (например, на основании усреднения двух предыдущих показателей). Данные величины

используются в качестве ограничений, определяющих потенциальное состояние элемента ЭА.

В случае, когда получить количественную оценку влияния ДФ не предоставляется возможным, на основе экспертной оценки происходит «принятие» или «непринятие» данного ДФ для ЭА. По существу это означает логическое условие: «ДФ влияет на ЭА» или «ДФ не влияет на ЭА».

4. Выбирается основной показатель модели катастрофоустойчивости ЭА, расчет которого позволяет характеризовать устойчивость ЭА в целом.

Объектом оценки уровня катастрофоустойчивости является ЭА в целом, поэтому в качестве основного показателя может быть выбран, например, коэффициент доступности информационных ресурсов ЭА, характеризующий степень доступности (или процент доступных) информационных ресурсов для конечных пользователей системы. В модели может быть определен ряд «критических» информационных ресурсов, отсутствие доступа к которым (хотя бы в течение какого-то непродолжительного времени) приводит к невозможности своевременного выполнения ЭА своих функций.

Поскольку одним из основных показателей, характеризующих информационную систему, является: $P(T_{ФУНК} \le T_Д)$ — своевременность, определяемая вероятностью выполнения системой своих функций за время, не превышающее $T_Д$ (директивно задано), то в качестве основного показателя может быть выбрано время восстановления после катастрофы ($T_{В.К.}$) с оценкой вероятности его выполнения $P(T_{В.К} \le T_{ДВ.К.})$, исходя из вышеизложенных предположений и допущений. $T_{ДВ.К.}$ — директивно заданное время восстановления после катастрофы. Допущением при этом является то, что средства резервирования выполнят свои функции в случае отказа основных средств ЭА.

Аналогичный показатель катастрофоустойчивости может быть при необходимости создан для каждого элемента или узла ЭА.

5. Выбираются дополнительные (частные) показатели катастрофоустойчивости ЭА. На их основе вычисляется основной показатель катастрофоустойчивости, или же частные показатели выступают в качестве ограничений к основному. К таким показателям можно отнести, например:

- коэффициент энергетической безопасности ЭА;
- коэффициент пожаробезопасности ЭА;
- коэффициент террористической безопасности ЭА;
- коэффициент отказоустойчивости ЭА (могут использоваться коэффициенты готовности, оперативной готовности, доступности);
- предельная пропускная способность информационных каналов ЭА;
- коэффициент климатической устойчивости ЭА (изменения климата);
- коэффициент информационной безопасности ЭА;
- коэффициент оперативности управления функционированием ЭА;
- показатели эффективности (качества) функционирования ЭА (например, полнота, достоверность, своевременность выполнения функций ЭА).

Состав показателей может дополняться и изменяться применительно к конкретному ЭА.

6. Разрабатываются модели расчета показателей катастрофоустойчивости (основного и частных) в зависимости от принципа функционирования элементов ЭА и моделей ДФ.

В общем случае ЭА может представлять собой иерархическую информационную систему: головной ЦОД с БД, региональный, районные ЦОД, каналы связи центр-регион, регион-район и т. д. Поэтому основной показатель для ЭА в целом рассчитывается на основе показателей элементов с применением весовых коэффициентов, обозначающих критичность элемента (например, по количеству обслуживаемых пользователей, катастрофоустойчивости элемента, ценности хранящейся информации и т. д.). Для приведенной выше формулы (1), критичность головного ЦОД (b_1) будет определяться как 1, критичность регионального ЦОД (b_{2i}) как, например, отношение ценности документов ЦОД к общей ценности документов ЭА и т. д.

Основной показатель катастрофоустойчивости может быть рассчитан как статический или как изменяющийся в зависимости от времени (например, как коэффициент оперативной доступности информационных ресурсов ЭА в произвольный момент времени и в течение заданного промежутка времени после него).

7. Модели снижения влияния ДФ на работу ЭА.

Для каждого вида ДФ разрабатываются модели контрмер, например, на основе собранной статистики или анализа причин возникновения ДФ.

При составлении модели должны быть учтены «стоимость» контрмер и оценка «остаточного влияния» ДФ на ЭА в случае принятия данных контрмер. В качестве критерия достаточности контрмеры в модели может выступать соотношение «стоимость/эффективность».

Необходимо провести ранжирование объектов ЭА по степени катастрофоустойчивости для:

- составления точной модели оценки вероятности восстановления ЭА после катастрофы;
- достаточности контрмер противодействия ДФ.

Ранжирование объектов ЭА предполагает два взаимосвязанных процесса:

– анализ уязвимости элементов ЭА;
– оценка катастрофоустойчивости конкретных элементов ЭА.

Анализ уязвимости элементов ЭА должен проводиться для наиболее важных (опасных) по степени угроз катастроф:

– по максимальным нематериальным потерям;
– по источнику наибольших материальных потерь;
– по источнику наибольших потерь ценной информации (электронных документов);
– по наиболее вероятным угрозам.

Анализ катастрофоустойчивости элементов ЭА должен выявить основные критические элементы, которые под воздействием катастроф и их последствий выходят из строя, теряют работоспособность, что приводит к отказу фрагмента ЭА или всего ЭА в целом. При необходимости вносятся поправки в модель катастрофоустойчивости в части нормирующих коэффициентов важности элементов ЭА (b_1, b_2, b_3 и т. д.).

Необходимо выделить факторы, которые негативно влияют на эффективность функционирования элементов ЭА. Такими факторами могут быть, например, следующие:

– отключение электропитания;
– нарушение условий функционирования средств ЦОД, ОКС (повышенная влажность, недопустимые колебания температуры, механические повреждения);
– нарушение условий хранения электронных документов;
– отсутствие ЗИП и обменного фонда;
– нарушение условий для осуществления обслуживающим персоналом своих функций;
– опасность для жизни обслуживающего персонала ЭА.

Таким образом, анализируя воздействие катастроф на критические элементы ЭА, можно отметить, что его уязвимость зависит от мощности (категории) катастрофы и наличия средств, нейтрализующих негативные факторы: как средств, находящихся на элементе ЭА, так и возможностей оперативной (в течение определённого времени, не превышающего $T_{ДВ.К.}$) ликвидации последствий катастрофы.

В общем случае математическая модель катастрофоустойчивости ЭА может быть представлена в виде:

$B = F(P_k,\ R_{нм},\ R_м,\ P_{вэ},\ N)$, где

B – уровень катастрофоустойчивости;

P_k – вероятность реализации мер противодействия катастрофе;

$R_{нм}$ – оценка нематериального ущерба;

$R_м$ – оценка материального ущерба;

$P_{вэ}$ – вероятность выхода из строя или потери критической информации;

N – функция влияния имеющихся средств и контрмер снижения уязвимости (в простейшем случае определяет наличие связанных с элементами и узлами средств и контрмер по отношению к каждому ДФ).

8. На основании частных моделей ДФ, противодействия ДФ, функционирования ЭА создается общая модель катастрофоустойчивости ЭА. Далее проводятся оперативные расчеты уровня катастрофоустойчивости и определяются стратегии повышения защищенности элементов ЭА.

Должна быть разработана методология периодической оценки влияния ДФ. Разрабатываемая методология должна позволять быстро и эффективно оценивать влияние ДФ и определять степени катастрофоустойчивости ЭА. Данная методология должна позволять вводить новые ДФ, включая разработку критериев для них, способ сбора данных, способ оценки влияния ДФ и описания модели влияния ДФ на ЭА.

Хорошим вариантом проведения полноценного моделирования катастрофоустойчивости ЭА является создание ситуационно-аналитического центра, реализующего модели функционирования ЭА и воздействий ДФ на систему (см. [17]). Их использование значительно повышает эффективность функционирования и развития информационных систем в целом, однако такие центры являются очень «дорогим удовольствием» и еще больше увеличивают избыточность ПТС ЭА.

Заключение

Тема исследования, затронутого в данной статье, является весьма актуальной, поскольку электронные документы (по факту в ПФ РФ, ФНС и др.) начинают активно замещать документы бумажные. Общая тенденция развития ПТС в мире говорит о том, что в ближайшее время вытеснение бумажных документов станет массовым явлением, и подходы к их безопасному хранению должны быть выработаны уже сейчас. При длительных сроках хранения тем более должна быть обеспечена катастрофоустойчивость решения ЭА, связанного с хранением электронных документов, представляющих большую ценность.

Для ЭА, работа которых связана с хранением ценных и особо ценных документов, утрата которых может вызвать невосполнимые материальные и/или нематериальные (политические, имиджевые и т. д.) потери, необходимо уделять большое внимание степени защищенности ЭА от катастрофических воз-

действий не только природного, но и техногенного, и антропогенного характера. В частности, общепризнано, что основные проблемы создания и внедрения информационных технологий в больших организационных системах сопряжены с влиянием человеческого фактора [3, 6–9]. Это еще раз подчеркивает, что система обеспечения катастрофоустойчивости ЭА должна быть всесторонне продумана, чтобы избежать неучтенных рисков с одной стороны и неоправданных затрат с другой. Необходима разработка модели катастрофоустойчивости ЭА, ее проверка и совершенствование, тщательное исследование результатов моделирования. Постоянный мониторинг на основе созданных моделей уровня защищенности ЭА.

Описанный в статье методологический подход к моделированию катастрофоустойчивости ЭА был разработан для оценки больших территориально-распределенных информационных систем и применялся при выполнении работ по повышению катастрофоустойчивости Государственной автоматизированной системы Российской Федерации «Выборы» [18].

Данная статья предназначена для систематизации и передачи знаний и опыта, полученных при разработке архивных систем, в частности, Электронных архивов долговременного хранения документов для Пенсионного фонда РФ (в эксплуатации с 2001 г., сроки хранения документов от 5 до 100 лет в зависимости от типа сведений), АКБ «Газпромбанк» (в эксплуатации с 1997 г., сроки хранения — десятки лет), коммерческих и государственных предприятий.

Предлагаемый в статье методологический подход может применяться не только к архивным решениям по долговременному хранению электронных документов, но и к решению проблем катастрофоустойчивости широкого класса информационных систем. Данный подход предполагает избыточность ПТС ЭА, дополнительные временные затраты при проектировании на составление моделей, дополнительные затраты для хранения «истории» функционирования ЭА, описание ДФ и элементов ЭА. Однако, по мнению авторов статьи, это необходимо и оправдано для обеспечения сохранности ценных электронных документов.

Литература

1. *Акимова Г. П., Пашкин М. А., Пашкина Е. В., Соловьев А. В.* Архивные хранилища и электронные архивы документов, основные постулаты и проблемы разработки // Труды Института системного анализа РАН (ИСА РАН). Т. 62. Вып. 4. М.: Красанд/URSS, 2012. С. 3–13.
2. ГОСТ Р 54989–2012 /ISO TR 18492:2005 Обеспечение долговременной сохранности электронных документов (вступает в силу с 01.05.2013).
3. *Дружинин Г. В.* Человек в моделях технологий. Часть I: Свойства человека в технологических системах. М.: МИИТ. 1996. 124 с.
4. *Акимова Г. П., Соловьев А. В.* Методология оценки надежности иерархических информационных систем // Системный подход к управлению информацией / Труды ИСА РАН. Т. 23. М.: КомКнига/URSS, 2006. С. 18–47.
5. *Акимова Г. П., Соловьев А. В., Янишевский И. М.* Методология оценки эффективности иерархических информационных систем // Системный подход к управлению информацией / Труды ИСА РАН. Т. 23. М.: КомКнига/URSS, 2006. С. 48–66.
6. *Цибулевский И. Е.* Ошибочные реакции человека-оператора. М.: Сов. радио, 1979. 208 с.
7. *Киреенко В. Е.* Человеческий фактор корпоративных информационных систем (на примере Томского горисполкома) // Вестник Томского государственного университета. № 275, апрель 2002 г.
8. *Ветлугин К.* Человеческий фактор // Computerworld 2006. № 11.
9. *Акимова Г. П., Соловьев А. В., Пашкина Е. В.* Методологический подход к определению влияния человеческого фактора на работоспособность информационных систем // Информационно-аналитические аспекты в задачах управления / Труды ИСА РАН. Т. 29. М.: Издательство ЛКИ/URSS, 2007. С. 102–112.
10. Научно-технический отчет. Совершенствование и доработка методического аппарата для оценки эффективности функционирования КСА ГАС «Выборы». М.: ИСА РАН, 2004.
11. *Завгородний В. И.* Комплексная защита информации в компьютерных системах. М: ВА РВСН им. Петра Великого, 1999.
12. ГОСТ Р51275–99 Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
13. *Постон Т. и Стюарт И.* Теория катастроф и ее приложения. М.: Мир, 1980.
14. *Касти Дж.* Большие системы. Связность, сложность и катастрофы. М.: Мир, 1982.
15. *Герасименко А.* Защита машин от биоповреждений. М.: Машиностроение, 1984.
16. Актуальные проблемы регулирования природной и техногенной безопасности в XXI веке. // Материалы десятой Международной научно-практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций. 19–21 апреля 2005 г. / МЧС России. М.: Ин-октаво, 2005. 400 с.
17. *Акимова Г. П., Соловьев А. В., Пашкина Е. В.* Ситуационно-аналитические центры, как способ снижения влияния человеческого фактора на принятие управленческих решений при эксплуатации больших информационных систем // Информационно-аналитические аспекты в задачах управления / Труды ИСА РАН. Т. 29. М.: Издательство ЛКИ/URSS, 2007. С. 113–122.

18. *Акимова Г. П., Пашкина Е. В., Соловьев А. В.* Методологический подход к моделированию поведения информационных систем при воздействиях катастрофического характера // Обработка изображений и анализ данных. Труды ИСА РАН. Т. 38. — М.: Книжный дом «Либроком»/URSS, 2008. С. 62–72.

19. *Акимова Г. П., Пашкин М. А., Пашкина Е. В., Соловьев А. В.* Электронные архивы: возможные решения проблем долгосрочного хранения данных / Труды Института системного анализа РАН (ИСА РАН). Т. 63. Вып. 4. С. 39–49.

Акимова Галина Павловна. Вед. н. с. ИСА РАН. К. т. н. Окончила в 1978 г. МФТИ. Количество печатных работ: 54. Область научных интересов: системное программирование, системный анализ, информационные технологии, влияние человеческого фактора, информационно-аналитические системы, электронный документооборот, электронный архив. E-mail: galina@cs.isa.ru

Пашкин Матвей Александрович. Н. с. ИСА РАН. Окончил в 2001 г. МГТУ «Станкин». Количество печатных работ: 13. Область научных интересов: системное программирование, информационные технологии, информационно-аналитические системы, электронный архив. E-mail: matveyp@cs.isa.ru

Пашкина Елена Владимировна. Н. с. ИСА РАН. Окончила в 2003 г. МГУ. Количество печатных работ: 9. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: alena@cs.isa.ru

Соловьев Александр Владимирович. В. н. с. ИСА РАН. К. т. н. Окончил в 1994 г. МГТУ им. Н. Э. Баумана. Количество печатных работ: 41. Область научных интересов: системный анализ, системы управления базами данных, теория надежности, влияние человеческого фактора, математическое моделирование, электронный документооборот. E-mail: alexsol@cs.isa.ru

Соловьев Дмитрий Валентинович. Н.с. ИСА РАН. Окончил в 1990 г. МФТИ. Количество печатных работ: 5. Область научных интересов: системный анализ, системы управления базами данных, методы управления проектами, влияние человеческого фактора, электронный документооборот. E-mail: sol@cs.isa.ru