

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.094



DOI: 10.21822/2073-6185-2024-51-4-99-111

Оригинальная статья / Original article

Показатели безопасности для современных систем электронного документооборота
И.И. Лившиц

Национальный исследовательский университет ИТМО,
197101, г. Санкт-Петербург, Кронверкский пр., д. 49, Россия

Резюме. Цель. В современных системах электронного документооборота (СЭД) обеспечивается управляемое движение множества документов по различным маршрутам. Успешное функционирование СЭД в значительной мере определяется доступностью конкретного документа в нужное время для определенного пользователя. Целью исследования является разработка математической модели СЭД, позволяющей определять показатель доступности ЭД с учетом УБИ и выполнять оптимизацию с учетом сложной организационной структуры современных организаций. **Метод.** Исследование проведено с помощью аппарата марковских процессов и формирования численных показателей безопасности. Особое внимание уделяется расчетам численного показателя доступности, позволяющего не только определять эффективность комплекса действующих мер защиты, но и количественно обосновывать требования ко времени обработки электронных документов. **Результат.** Определен важный атрибут – доступность, численный показатель которого позволяет оценивать общий уровень конкретной СЭД и одновременно решать множество частных задач выявления и противодействия угрозам блокирования информации, злонамеренной задержки согласования, отклонения от установленных маршрутов, что напрямую влияет на доступность и, соответственно, на общий уровень безопасности. **Вывод.** Известные типы применяемых моделей (функциональный, теоретико-множественный, теоретико-графовый, вероятностно-параметрический) не позволяют явно формировать оценки доступности. Предложенная модель позволяет идентифицировать уязвимости в СЭД, которые могут быть использованы для реализации новых УБИ и содействовать повышению уровня обеспечения ИБ в проектах СЭД.

Ключевые слова: электронный документ, система электронного документооборота, метрики безопасности, риски, остаточные риски, информационная безопасность, доступность, оптимизация

Для цитирования: И.И. Лившиц. Показатели безопасности для современных систем электронного документооборота. Вестник Дагестанского государственного технического университета. Технические науки. 2024;51(4):99-111. DOI:10.21822/2073-6185-2024-51-4-99-111

Security indicators for modern electronic document management systems

I.I. Livshits

National Research University ITMO,
49 Kronverksky Ave., St. Petersburg 197101, Russia

Abstract. Objective. Modern electronic document management systems (EDMS) provide controlled movement of multiple documents along different routes. Successful functioning of EDMS is determined by the availability of a specific document at the right time for a specific user. The purpose of the study is to develop a mathematical model of EDMS that allows determining the indicator of ED availability taking into account the UBI and performing optimization taking into account the complex organizational structure. **Method.** The study was conducted using the apparatus of Markov processes and the formation of numerical safety indicators.

Particular attention is paid to the calculations of the numerical indicator of availability. **Result.** An important attribute has been determined - availability, the numerical indicator of which allows assessing the general level of a specific EDMS and simultaneously solving many specific problems of identifying and countering threats of information blocking, malicious delay in approval, deviation from established routes, which affects availability and, accordingly, the overall level of security. **Conclusion.** Known types of applied models (functional, set-theoretic, graph-theoretic, probabilistic-parametric) do not allow explicitly forming availability assessments. The proposed model allows identifying vulnerabilities in the EDMS, which can be used to implement new UBI and contribute to increasing the level of information security in EDMS projects.

Keywords: electronic document, electronic document management system, security metrics, risks, residual risks, information security, availability, optimization

For citation: I.I. Livshits. Security indicators for modern electronic document management systems. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(4):99-111. DOI:10.21822/2073-6185-2024-51-4-99-111

Введение. В настоящее время многие компании реализуют масштабные программы по внедрению СЭД [1,2]. Известно, что при эксплуатации СЭД объективно требует не только обработка значительного количества электронных документов (ЭД), но и обеспечение заданного уровня ИБ. Требования ИБ обусловлены тем фактом, что из-за объективных недостатков реализации управляемых информационных потоков (УИП) возможна реализация рисков доступности, соответственно, часть ЭД может не быть обработана в заданное (целевое) время [3]. Следует признать, что внимание к реализации требований ИБ является в настоящее время объективно важной и актуальной проблемой, поскольку постоянно обнаруживаются новые и новые угрозы безопасности информации (далее – УБИ), в самых различных реализациях СЭД.

Постановка задачи. Для целей обеспечения ИБ в современных СЭД крайне важно обратить внимание на качество разработки и реализации маршрутов движения ЭД и оптимизации системной логики обработки, т.е. от «качества» практической реализации СЭД объективно зависит эффективность управленческой деятельности компании в целом. Для конкретной компании, «включившей» в состав корпоративного ИТ-ландшафта СЭД, задача анализа особенностей движения ЭД в аспекте ИБ приобретает исключительную важность: ущерб при нарушении бесперебойного движения ЭД может быть значительным, вплоть до полного блокирования нормального функционирования (известны примеры критических сбоев СЭД Росавиации и ФТС [13, 14]). В типовой СЭД определенный ЭД недоступен пользователю, пока не поступит конкретная задача его обработки. При наличии отклонений, вызванных различными УБИ, конкретный ЭД может не достигнуть точки назначения по маршруту в заданное (расчётное) время. В связи с этим в типовой СЭД может нарушаться важное свойство ИБ – доступность (в соответствии с требованиями известных стандартов ГОСТ Р ИСО/МЭК 27001-2021 или ISO/IEC 27001:2022). Из указанного положения логично следуют требования к обеспечению всех аспектов безопасности, предъявляемые к такому объекту, как СЭД. В определенном смысле (например, в соответствии с указанными выше стандартам ГОСТ Р ИСО/МЭК), можно говорить о «результативности», как способности СЭД достигать заданных целей ее создания. Безопасная СЭД должна не только автоматизировать движение ЭД, но и обеспечивать достижение результата с точки зрения выбранного критерия (критериев) по определенным маршрутам. В этом аспекте представляется обоснованным обратить внимание на оптимизационные задачи, связанные с нахождением оптимальных путей прохождения (маршрутов) ЭД в СЭД и гарантирующих успешное достижение финальной точки. В представленной публикации предлагается для СЭД применять новый критерий безопасности – численную оценку вероятности достижения ЭД заданного маршрута [4].

Анализ литературы [5-11] показал, что вопрос эффективного управления информационными потоками ЭД изучен не в полной мере. Известно, что к настоящему моменту времени существует достаточно методов моделирования СЭД, начиная с теоретико-множественных, теоретико-графовых подходов и заканчивая моделями на сетях Петри. Следует отметить, что схожие модели используются в иных предметных областях, например, при решении транспортных и логистических задач, управления задачами в центрах обработки данных и др. В то же время, обоснованной математической модели СЭД, которая позволила бы оптимизировать движение ЭД с учетом критериев ИБ (конкретно – доступности), в опубликованных работах не представлено. Применение методов математического моделирования может быть обосновано комплексом преимуществ – получением численных значений, позволяющих оптимизировать варианты реализации мероприятий по ИБ, известной практикой программной реализации, возможностью верификации полученных результатов. Представленная статья состоит из краткого обзора применяемых моделей известных подходов (функционального, теоретико-множественного, теоретико-графового, вероятностно-параметрического), описания математической модели СЭД, формирования задачи оптимизации и примера численного расчета с использованием системы уравнений Колмогорова.

Целью настоящего исследования является разработка математической модели для оценки безопасности СЭД с учетом УБИ в отношении доступности ЭД и показателей безопасности для современных СЭД.

В работе Круковского М.Ю. [4] рассматривается подход к созданию моделей композитного документооборота на основе аппарата теории графов. Описаны методы определения множеств для разработанной модели, предложена алгебра документооборота с использованием графов. Положения этих работ могут быть использованы для дальнейшего развития теории и практики электронного документооборота и создания на их основе прикладного программного обеспечения. В работе [5] предложена модель, описывающая организационную структуру, как упорядоченное множество элементов структуры предприятия – подразделений и функциональных служб; а также процессы, протекающие в системе управления по элементам в составе деятельности по осуществлению функций управления. Достаточно интересно описана организационная культура, характеризующая уровень отношения в организации к так называемым структурообразующим документам.

В работе [6] представлена модель в нотации eEPC (*extended Event Driven Process Chain*), в которой определены множества объектов: типа I, которое состоит из элементов I_{pos} и I_{org} , где: I_{pos} – множество объектов типа «Должность»; I_{org} – множество объектов типа «Организационная единица», соответственно; типа D, которое состоит из элементов D_{doc} и D_{inf} , где: D_{doc} – множество объектов типа «Документ», D_{inf} – множество объектов типа «Информационный объект», соответственно. Представленная работа дает хороший аналитический базис в известной функциональной нотации, но без принятия во внимание аспектов обеспечения безопасности движения ЭД в СЭД.

В работе [7] рассматриваются информационные системы юридически значимого электронного документооборота в структуре управления Вооруженными силами Российской Федерации. Разработана математическая модель процесса обеспечения технической и юридической целостности ЭД и представлена модель УБИ, вызванных внутренними и внешними факторами. В указанной работе применяется логико-вероятностный метод И.А. Рябины, позволяющий получать численные значения вероятностей перехода информационных систем в опасное состояние с учетом структуры таких систем. В работе [8] рассматриваются формальные системы математической логики, в том числе система алгебры конечных предикатов, применительно к решению задач ЭДО. Предложен вывод о необходимости описания процессов в СЭД на языке теорий математической логики, позволяющих учитывать не только содержание, но и структуру

формализованного ЭД. Сделаны выводы о том, что применение логических моделей позволяет снизить затраты на вычислительные мощности и сократить машинное время обработки ЭД, но вопросы обеспечения ИБ в СЭД не рассматриваются.

Публикация [9] по мнению автора по праву является классическим трудом в области создания математических моделей с ключевым вниманием к оценке эффективности защиты от УБИ по отношению к полной «триаде» ИБ: целостности, доступности и конфиденциальности ЭД. В указанной работе учитывается также длительность жизненного цикла (ЖЦ) в отношении ЭД для СЭД. Математическое моделирование процессов СЭД и реализации УБИ выполнено с использованием аппарата сетей Петри-Маркова. В работе [10] рассматриваются проблемы документационного сопровождения управленческого решения, а также описываются технологии и модели организации документооборота. Представлены методы и алгоритмы принятия решения при организации контроля, но конкретные детали процессов обеспечения ИБ в СЭД не рассматриваются; представлена математическая модель динамики функционирования подсистемы защиты конфиденциальных сведений в СЭД. Модель разработанная на основе графовой формализации с использованием аппарата сетей Петри и матрицы вероятностно-временных характеристик переходов между состояниями функционирования системы. Существенным отличием данной публикации является описание динамики функционирования подсистемы защиты конфиденциальных сведений. В работе Краснянского М.Н. [11] исследуются математические модели обработки информации в СЭД. Предложенные модели используются для формализации структуры ЭД, оптимизации процессов их обработки, взаимодействия и движения.

В работе представлен теоретико-множественный анализ процессов обработки информации и реализация в алгоритмическом и программном обеспечении. Вопросы обеспечения ИБ в СЭД в упомянутой работе не рассмотрены.

Методы исследования. В рамках функциональной модели предлагается следующая последовательность действий для анализа эффективности СЭД. В практическом аспекте предлагается для реализации высокоуровневая схема моделирования УИП в типовой СЭД (рис. 1).

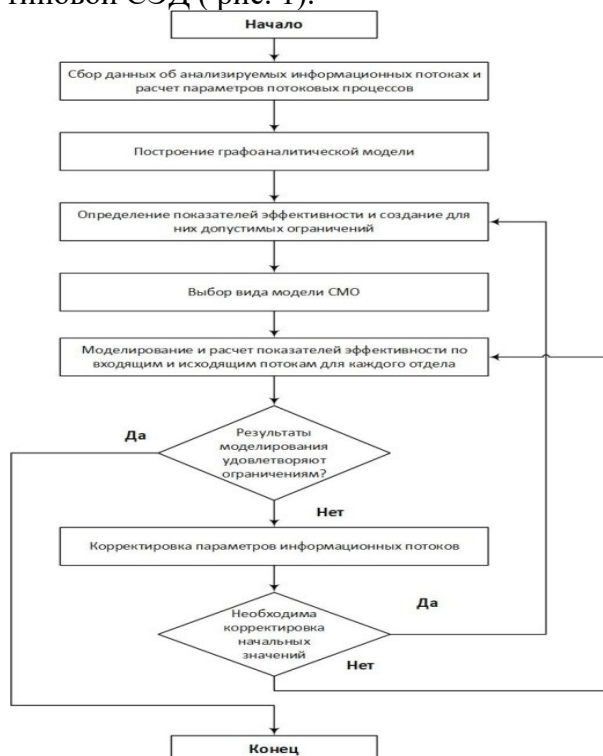


Рис. 1. Высокоуровневая схема моделирования УИП в СЭД

Fig. 1. High-level scheme of modeling UIP in the ECM

Описанная выше схема отличается универсальностью и упрощает дальнейший процесс моделирования, так как формирует единое представление о движении УИП в конкретной СЭД. Явным достоинством данной модели является учет типа ЭД – этот параметр может внести позитивный вклад при локализации «узкого» места при оптимизации маршрутов ЭД в СЭД. Необходимо отметить, что в аспекте поставленной задачи оценки безопасности СЭД (конкретно – доступности), рассмотренная выше схема в терминах теории множеств требует существенных доработок. Например, хотя в алгоритме анализа и моделирования УИП предусмотрено задание допустимых ограничений и последующее их сравнение с реальными показателями, в рассматриваемой схеме для учета отклонений не введены важные план-фактные переменные.

Кроме того, как показала практика, ограничения следует устанавливать не только на показатели эффективности, но и на маршрутные показатели следования конкретного ЭД, минимально для идентификации его «обратного» движения или заикливания. Таким образом, в текущем виде базовая теоретико-множественная модель не может быть эффективно использована при решении задачи обеспечения безопасности СЭД, так как не отражает всех требований к доступности ЭД. В то же время предложенная графоаналитическая модель может быть практически применена для целей обеспечения безопасности СЭД, поскольку позволяет дополнительно наглядно отобразить взаимодействие подразделений (конкретных исполнителей) и оценивать эффективность маршрутов движения ЭД в аспекте оценки доступности. Тем не менее, существенные ограничения должны быть приняты при проектировании новых СЭД и/или оптимизации существующих – в отношении реализации временной шкалы, что является предметом исследования представленной публикации. Крайне важно, что применение подходов, использующих экспертные процедуры оценивания уровня ИБ в СЭД, но не учитывающих временной фактор, могут приводить к неполной, и даже к некорректной оценке.

Теоретико-множественный подход. Описание в терминах теории множеств для исходящих и входящих УИП приводится в [5], где теоретико-множественная модель представляется следующим образом:

$$S_i = \langle \{L_{ij}\}, \{T_{ij}\} \rangle,$$

где: S_i – определение конкретного подразделения, УИП которого исследуются; $\{L_{ij}\}$ – множество входящих документов для выбранного i -го подразделения, поступающих из j -го подразделения; $\{T_{ij}\}$ – множество исходящих документов, направляемых из текущего i -го подразделения для j -ого подразделения.

Представленная модель на соответствующих уровнях организационной структуры конкретной организации отображает меру взаимодействия между подразделениями $S_0, S_1, \dots, S_n$. Для целей данной публикации отметим, что преимуществом модели [5] является возможность оценивания эффективного распределения нагрузки между различными категориями исполнителей.

Теоретико-графовый подход. Теоретико-графовый подход описан в [4]. В соответствии с этим подходом СЭД представлена как совокупность упорядоченных действий, реализуемых множеством конкретных исполнителей над множеством определенных ЭД:

$$\text{ФМД} = \{И; Д; С\},$$

где: ФМД – формальная модель документооборота; И – множество исполнителей; Д – множество действий, С – множество состояний.

Конечная совокупность дискретных представлений конкретного ЭД в пределах его ЖЦ определяется множеством состояний. Логика документооборота представляется в виде последовательности определенных действий, которые приводят конкретный ЭД (как объект управления) к смене одного из определенных состояний на другое, соответственно, описывается «следование» определённого ЭД по конкретному маршруту из начального (исходного) состояния в требуемое (конечное). Теоретико-графовую

модель можно также определить на основе применения матрицы инцидентности, которая определяет общую теоретико-графовую модель СЭД для рассматриваемого конкретного бизнес-процесса. Модели такого типа подходят для обнаружения отклонений в заданном маршруте следования ЭД [7,8]. Целесообразно отметить, что построение матрицы инцидентности и ее анализ придется выполнять для каждого ЭД в отдельности, что может потребовать избыточных вычислительных ресурсов для СЭД крупной компании.

Вероятностно-параметрический подход. Сеть Петри-Маркова может быть формально представлена в виде [9]: $\theta = \langle \Pi, M \rangle$,

где: Π – сеть Петри, определяющая структуру сети Петри-Маркова, M – случайный процесс, накладываемый на структуру Π .

Рассматриваемая модель [9] позволяет обеспечить расчет среднего времени обработки конкретных ЭД, кроме того, расчеты строятся на основе структурно-операционной модели процесса обработки конкретного ЭД (рис. 2).

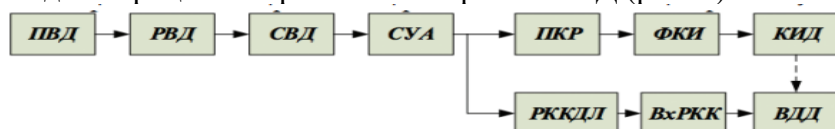


Рис. 2. Структурно-операционная модель процесса обработки ЭД
Fig. 2. Structural and operational model of the ED processing process

На рис. 2 обозначены процедуры: ПВД – приема входящего ЭД; РВД – регистрации входящих документов; СВД – сканирования входящего ЭД; СУА – создания уведомления адресата; ПКР – подготовки карточки резолюции; ФКИ – формирования карточки исполнения; КИД – контроля исполнения документа; РККДЛ – создания регистрационно-контрольной карточки исходящего документа; ВхРКК – создания регистрационно-контрольной карточки входящего документа; ВДД – вывода документа из действия.

На основании конкретных траекторий движения ЭД, а также учитывая среднюю длительность исполнения каждой функции по конкретной траектории, в рассматриваемой модели формируют оценку среднего времени исполнения конкретного ЭД, которую затем применяют в показателях оценки эффективности системы ИБ в конкретной реализации СЭД [9]. Определим ограничения: длительность ЖЦ i -го ЭД объективно является случайной величиной, которая зависит от множества факторов (например, количество процедур обработки конкретного ЭД, объем рассматриваемого ЭД, квалификация (мотивация) назначенных исполнителей и т.д.). Предложенная модель на сетях Петри-Маркова соответствует реальным УИП в СЭД и будет рассмотрена далее при формировании новой модели СЭД. Уместно заметить, что в известных источниках не рассматривается риск-ориентированный подход, позволяющий оценить возможный ущерб нарушения нормального движения ЭД в корпоративных СЭД с последующим нарушением их доступности [5].

Математическая модель СЭД с использованием аппарата марковских процессов. При рассмотрении процессов в СЭД целесообразно представлять процессы движения ЭД таким образом, что переходы объектов (ЭД) из состояния в состояние происходят под действием потоков событий. В терминах потока событий возможно описать поток ЭД, связанных с определенным бизнес-процессом, поскольку:

1. Поток ЭД, перемещающихся из состояния в состояние, возможно рассматривать как стационарный на интервалах рабочего времени, установленного в компании, благодаря тому что вероятностные характеристики такого потока на указанных промежутках времени не меняются;
2. События, образующие поток, появляются в последовательные моменты времени независимо (сотрудники запускают один и тот же бизнес-процесс независимо друг от друга, например, запуск заявок на командирование);

3. Вероятность «попадания» на заданный интервал времени двух или более событий пренебрежимо мала по сравнению с вероятностью «попадания» одного события, иными словами, поток ординарен.

Соответственно, представляется целесообразным применить теорию дискретных марковских случайных процессов с непрерывным временем [12] для моделирования бизнес-процессов, в рамках которых функционирует конкретный экземпляр СЭД.

Для описания поведения реальной СЭД необходимо: определить все конкретные состояния, в которых может находиться рассматриваемая система; сформировать граф состояний, т.е. указать пути возможных переходов (маршрутов) системы из одного состояния в другое; определить начальное состояние рассматриваемой системы; сформировать матрицу интенсивностей переходов, иными словами, для каждого возможного перехода указать соответствующую интенсивность потока событий, переводящих систему из одного состояния в другое. Моменты возможных переходов в моделируемых бизнес-процессах СЭД из состояния в состояние случайны и происходят под действием событий, характеризующихся интенсивностям. Поскольку рассматривается движение значительного количества ЭД (несколько тысяч в месяц), для описания функционирования конкретной СЭД может быть применен эффективный метод динамики средних. Демонстрация модели на нескольких примерах представленной размерности (сотни маршрутов движения ЭД и тысячи ЭД в месяц) может считаться достаточным экспериментальным доказательством практической эффективности предложенного метода для оценки безопасности конкретной реализации СЭД. Соответственно, уравнения Колмогорова составляются относительно средних численностей (математических ожиданий) состояний исследуемых объектов.

Формализация задачи оптимизации функционирования СЭД. Принимая к исследованию функциональную модель СЭД [7], представим процессы обработки ЭД в виде графа состояний (рис. 3):

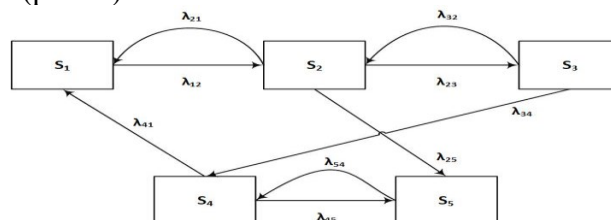


Рис. 3. Граф состояний функционирования СЭД
 Fig. 3. Graph of the functioning states of the ECM

ЭД может находиться в одном из 5 состояний: S_1 – подготовка ЭД; S_2 – согласование ЭД; S_3 – утверждение ЭД; S_4 – исполнение и контроль исполнения ЭД; S_5 – сдача ЭД в архив.

Задача оптимизации функционирования системы СЭД может быть сформулирована следующим образом:

$$F = C_3 m_3 + C_4 m_4 \rightarrow \max$$

Для стационарного режима вводятся следующие ограничения целевой функции:

$$m_1 + m_2 + m_3 + m_4 + m_5 = N$$

$$m_1(0) = N, m_1 \leq 100, m_2 \leq 90$$

где: C_3 (C_4) – стоимость нахождения системы в единицу времени в состоянии S_3 (S_4); m_j ($j=1...5$) – средняя численность элементов системы в j -ом состоянии; λ_{ij} ($i=1...5$) – интенсивность перехода элемента системы из i -го в j -ое состояние.

Критерий оптимальности затрагивает только состояния S_3 (S_4), таким образом, многокритериальная задача оптимизации функционирования СЭД может быть представлена как однокритериальная задача путем свертки критериев $C_i m_i$ по каждому оптимизируемому состоянию (S_i) в один. Выражение $m_1 + m_2 + m_3 + m_4 + m_5 = N$ и $m_1(0) = N$ являются нормирующими и определяют начальные условия решения

системы линейных алгебраических уравнений, а также общее количество ЭД в исследуемой СЭД. Соотношения $m_1 \leq 100$ и $m_2 \leq 90$ ограничивают максимальное количество ЭД в состояниях S_1 (S_2), и призваны сократить количество ЭД в «непродуктивных» состояниях. Оптимизацию предлагается производить как по средним численностям состояний ЭД – m_j ($j=1..5$), так и по интенсивностям переходов λ_{ij} . Выбор среди интенсивностей параметров управления зависит от рассматриваемой ситуации для «целевой» СЭД.

Построенная модель позволяет перейти к важной и актуальной задаче – формированию численной оценки рисков ИБ в СЭД (например, в соответствии с требованиями ГОСТ Р ИСО 31000–2019 или ISO 31000:2018). В рамках исследуемой задачи под оценкой риска понимается количественная оценка негативных последствий отклонения от запланированных переходов по фиксированному маршруту и негативное влияние на доступность ЭД. В рассматриваемом примере оценка объективно носит многокритериальный характер и, соответственно, определяется не в стоимостном выражении, а в условных единицах по 100-балльной шкале экспертным методом.

Уместно отметить несколько важных моментов, которые могут расширить применение данной работы:

- стандарты ГОСТ Р ИСО (ISO) серии 31000 предусматривают более 40 методов оценивания рисков, в том числе и быстрый эффективный метод экспертной оценки;
- результаты экспертных оценок данной работы подтверждаются независимыми внешними аудитами (обязательными для определенного типа компаний).

Анализ полученных результатов объективно поможет лицам, принимающим решения (ЛПР), сформировать конкретные и четкие рекомендации, основанные на оперативных, достоверных данных и успешно идентифицировать «узкие» места в функционировании конкретной СЭД для ее непрерывного совершенствования в аспекте ИБ. Поскольку интенсивность перехода из состояния в состояние обратна пропорциональна среднему времени перехода, для реализации оптимального решения ЛПР следует выяснить, какие факторы существенно влияют на время согласования конкретных категорий документов. Среди них могут быть, в частности: сложность процесса согласования, связанная с отсутствием типовых маршрутов, количество ЭД, низкая дисциплина сотрудников, недостаточная квалификация и мотивация персонала.

Уместно обратить внимание, что задача оптимизации функционирования СЭД напрямую связана с обеспечением доступности ЭД, что позволяет предоставить обоснованные численные оценки степени обеспечения ИБ. В частности, задачи оптимизации затрагивают все подразделения, «охваченные» СЭД, и позволяют определить обобщенный показатель доступности ЭД через понятие «петли» (как негативного влияния на расчетную доступность СЭД. Кроме того, учет множества факторов, влияющих на доступность ЭД позволит объективно вычислить общий показатель безопасности СЭД в конкретной реализации (в том числе с учетом реализованных мер ИБ). Для задачи оптимизации СЭД важно, что в каждой точке маршрута ЭД может находиться в одном из трех состояний – «Согласовано», «Согласовано с замечаниями», «Не согласовано». Входными данными для такой модели движения ЭД является точное понимание возможных переходов, которые необходимо смоделировать, а также вероятности перехода из одного состояния в другое, которые представляются в виде матрицы переходов и могут быть исчислены на основании статистического анализа движения конкретного типа ЭД в конкретной реализации СЭД, как показано выше.

Процесс согласования одного конкретного вида ЭД может быть представлен следующей моделью (рис. 4): Каждой цифре соответствуют следующие этапы согласования: 1 – согласование непосредственным руководителем; 2 – согласование в отделе №1; 3 – согласование в отделе №2; 4 – согласование в отделе №3;

5 – согласование в отделе № 4; 6 – согласование главным бухгалтером; 7 – согласование генеральным директором; 8 – получение результата «Согласовано»; 9 – получение результата «Не согласовано»; 10 – 13 – дополнительные согласования сотрудниками, ранее не предусмотренными в заданном маршруте («петли», лишняя «паразитная» работа).

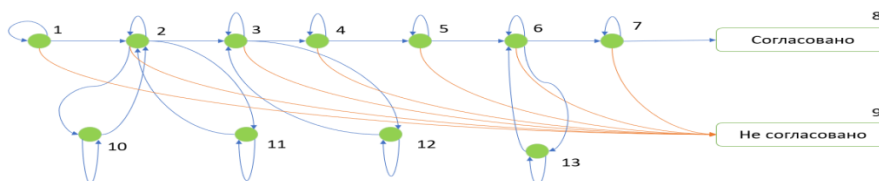


Рис. 4. Модель согласования конкретного вида ЭД
Fig. 4. Model of coordination of a specific type of ED

Обсуждение результатов. Экспериментальная оценка функциональной модели СЭД, представленной на рис. 3, определяет, что в каждую точку установленного маршрута конкретный ЭД приходит с одним из статусов – «Согласовано», «Согласовано с замечаниями», «Не согласовано» (например, $\lambda_{23}, \lambda_{25}, \lambda_{24}$ – интенсивности согласования документа Отделом №1, λ_{21} – интенсивность несогласования документа Отделом №1), как было показано ранее на рис. 4. Входными данными для представленной модели движения ЭД является точное понимание возможных переходов, которые необходимо смоделировать, а также интенсивности переходов из одного состояния в другое, которые могут быть исчислены на основании статистического анализа движения определенного типа ЭД в конкретной корпоративной реализации СЭД.

Такой вид модели имеет существенные преимущества:

1. Учитывает статистическую неопределенность времени обработки конкретного ЭД в определенном отделе: интенсивности переходов обратно пропорциональны среднему времени работы над конкретным видом ЭД;
2. Учитывает непредсказуемый порядок осуществления переходов между возможными состояниями: в частности, учитывается, что в любой момент времени конкретный ЭД может находиться на обработке в любом из отделов.

Анализ конкретного вида ЭД подразумевает под собой их большое количество, соответственно, необходимо возвратиться к методу динамики средних. Система дифференциальных уравнений Колмогорова, соответствующая графу состояний, представленному на рис. 3, относительно средних численностей состояний ЭД примет следующий вид:

$$\begin{cases} \frac{dm_1}{dt} = -m_1(\lambda_{12} + \lambda_{13} + \lambda_{14}) + m_2\lambda_{21} + m_3\lambda_{31} + m_4\lambda_{41} + m_5\lambda_{51} \\ \frac{dm_2}{dt} = -m_2(\lambda_{21} + \lambda_{23} + \lambda_{24} + \lambda_{25}) + m_1\lambda_{12} + m_3\lambda_{32} + m_4\lambda_{42} + m_5\lambda_{52} \\ \frac{dm_3}{dt} = -m_3(\lambda_{31} + \lambda_{32} + \lambda_{34} + \lambda_{35}) + m_1\lambda_{13} + m_2\lambda_{23} + m_4\lambda_{43} + m_5\lambda_{53} \\ \frac{dm_4}{dt} = -m_4(\lambda_{41} + \lambda_{42} + \lambda_{43} + \lambda_{45}) + m_1\lambda_{14} + m_2\lambda_{24} + m_3\lambda_{34} + m_5\lambda_{54} \\ \frac{dm_5}{dt} = -m_5(\lambda_{51} + \lambda_{52} + \lambda_{53} + \lambda_{54}) + m_2\lambda_{25} + m_3\lambda_{35} + m_4\lambda_{45} \end{cases}$$

Нормирующее условие: $m_1 + m_2 + m_3 + m_4 + m_5 = N$, где: N – количество документов конкретного вида. Матрица интенсивностей переходов представлена в табл. 1.

Таблица 1. Матрица интенсивностей переходов (количество/час)

Table 1. Transition intensity matrix (number/hour)

	S ₁	S ₂	S ₃	S ₄	S ₅
S ₁	0	0,2	0	0	0
S ₂	0	0	0,15	0	0
S ₃	0,15	0,7	0	0,7	0
S ₄	0,15	0	0,3	0	0,4
S ₅	0,3	0	0	0,2	0

При заданной матрице интенсивностей переходов и $N = 250$ (кол-во ЭД) получим решение системы дифференциальных уравнений при помощи Python (рис. 5).

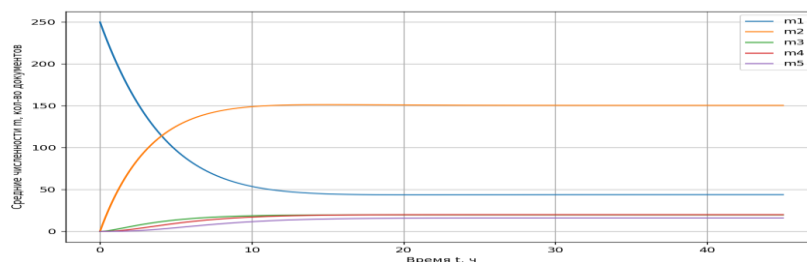


Рис. 5. Решение системы дифференциальных уравнений в Python

Fig. 5. Solving a system of differential equations in Python

В стационарном режиме система имеет вид:

$$\begin{cases} 0 = -m_1\lambda_{12} + m_3\lambda_{31} + m_4\lambda_{41} + m_5\lambda_{51} \\ 0 = -m_2\lambda_{23} + m_1\lambda_{12} + m_3\lambda_{32} \\ 0 = -m_3\lambda_{34} - m_3\lambda_{32} + m_2\lambda_{23} + m_4\lambda_{43} - m_3\lambda_{31} \\ 0 = -m_4\lambda_{41} - m_4\lambda_{45} + m_3\lambda_{34} - m_4\lambda_{43} + m_5\lambda_{54} \\ 0 = -m_5\lambda_{54} + m_4\lambda_{45} - m_5\lambda_{51} \end{cases}$$

Решение системы линейных алгебраических уравнений:

$$m_1 = 49; m_2 = 150; m_3 = 18; m_4 = 18; m_5 = 15$$

При имеющейся матрице интенсивностей переходов большое количество документов находится в Отделе №1 (рис. 3), значительная доля документов возвращается на доработку. Анализ системы в стационарном режиме позволяет объективно определить, где находятся «узкие места» в маршрутах согласования ЭД в корпоративной СЭД. Построенная модель позволяет перейти к численной оценке рисков ИБ в СЭД, что соответствует известному подходу ГОСТ Р ИСО серии 31000 и 27005.

В рамках решения задачи оперативного планирования СЭД, определено, для анализа процессов со стороны ЛПР, необходимы отчеты с объективными данными об исполнительской деятельности сотрудников за определенный период с полями, минимально: «Исполнитель», «Подразделение исполнителя», «Дата начала», «Результат задачи», «Плановая дата исполнения», «Фактическая дата исполнения», «Плановый срок», «Фактический срок», «Просрочка», «Факт-план», «Количество итераций».

В рамках рассматриваемой задачи оценка «Количество итераций» рассматривается как число дополнительных излишних («паразитных») циклов согласования ЭД. В аспекте ИБ излишние циклы согласования ЭД могут реализовываться как по заданным маршрутам, так и неуправляемо (в критичном случае – реализации УБИ) порождать новые маршруты движения ЭД, но в любом случае существенно влияют на доступность. Если количество итераций не равно нулю, следовательно, имело место быть обратное движение ЭД, а именно – «паразитная» работа (как было показано на рис. 4). Соответственно, для отслеживания временных отклонений в согласовании ЭД предлагается ввести дополнительные показатели «Отклонение» и «Наличие просрочки». В поле «Отклонение» подсчитывается разность между фактической датой исполнения ЭД и его плановой датой, в связи с чем значения в пределах данного поля могут быть как положительными (позднее исполнение), так и отрицательными (раннее исполнение).

Разработаем систему показателей для определения степени обеспечения ИБ и СЭД и, конкретно, заданной степени доступности. Для отражения факта достижения (недостижения) поставленных целей, выраженных количественно, введем метрики безопасности. Для этой цели предлагается руководствоваться стандартом ГОСТ Р ИСО/МЭК (ISO/IEC) серии 27004, где представлены рекомендации по разработке и использованию измерений в области ИБ, в том числе с учетом возможности оперативного анализа полученных результатов со стороны ЛПР. Примем во внимание набор анализируемых показателей степени обеспечения ИБ (метрик ИБ), в частности: процент несогласования, процент просрочек, наличие «паразитной работы»

(или «петель», как было показано на рис. 4), длительное согласование и занятость (непосредственно влияющих на доступность):

- процент несогласования – доля не согласованных исполнителем документов к общему числу рассмотренных;
- процент просрочек – доля документов с нарушенным сроком исполнения к общему числу документов, обработанных исполнителем;
- процент согласования – доля согласованных и согласованных с замечаниями исполнителем документов к общему числу рассмотренных;
- наличие «петель» – доля документов с любыми отклонениями от планируемых переходов по маршруту к общему числу документов исполнителя;
- занятость – общее количество документов, обработанных исполнителем за определенный временной промежуток.

Предложенные показатели СЭД могут быть наглядно представлены в виде системы отчетов. Например, полный анализ текущего состояния функционирования системы СЭД логически разделяется на три части – сравнение сотрудников выбранных подразделений по двум показателям с возможностью масштабирования (рис.6), сводка результатов согласования документов по выбранным подразделениям (рис.7) и ранжирование подразделений по одному предопределенному показателю (рис.8), соответственно. Дополнительные показатели ИБ позволяют ЛПР оперативно обнаружить тех сотрудников, которые являются лидерами в генерации «петель», например, в составе одного подразделения (рис. 6). Такой анализ, предпринятый своевременно, позволит существенно снизить риски доступности корпоративной СЭД, например, для выполнения крупного заказа или оценить уровень обеспечения ИБ до начала внешнего аудита по требованиям безопасности.

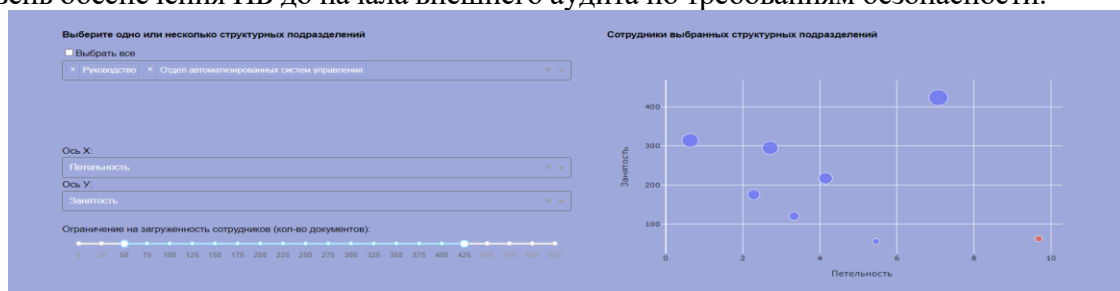


Рис. 6. Сравнение сотрудников подразделений по двум дополнительным показателям
Fig. 6. Comparison of department employees by two additional indicators

Аналогичные результаты на более высоком уровне иерархии могут быть сформированы в разрезе подразделений и определенных статусов ЭД, «проходящих» через них по установленным маршрутам (рис. 7).

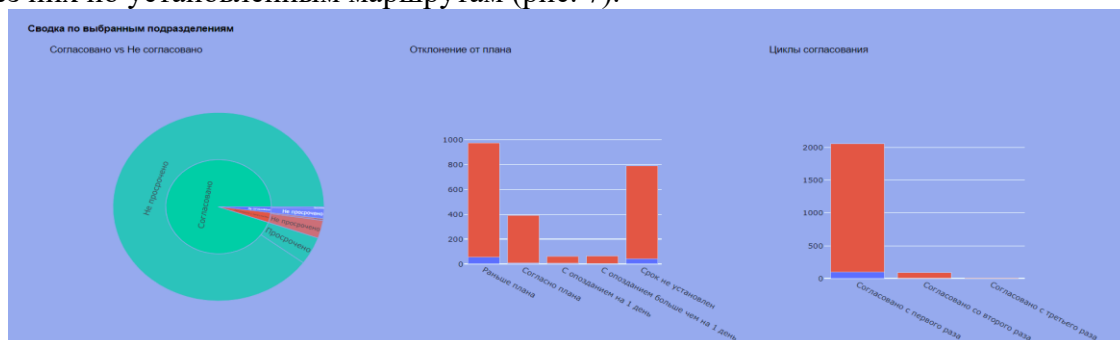


Рис. 7. Сводка по выбранным подразделениям
Fig. 7. Summary of selected departments

В аспекте обеспечения доступности эта аналитика позволяет оценить «загруженность» тех или иных служб, выявить «узкие места» и снизить риски срыва поставленных производственных задач в силу значительного количества избыточных («паразитных») циклов согласования. В определенном смысле этот отчет позволяет выявить подразделения,

имеющие критичное влияния на обеспечение доступности ЭД для всей компании (например, в силу монопольного ресурса на согласование финансовых лимитов). Для ЛПР крайне важно представление четких, измеримых и унифицированных показателей, например, аналитический срез по проценту несогласованных документов (рис. 8). В аспекте обеспечения ИБ этот дополнительный показатель может успешно решать обратную задачу – как «целевое» подразделение (например, отдел документационного обеспечения) обеспечивает фильтрацию недостаточно качественных документов (подготовленных «на авось»), прохождение которых через СЭД может нанести ущерб интересам организации.

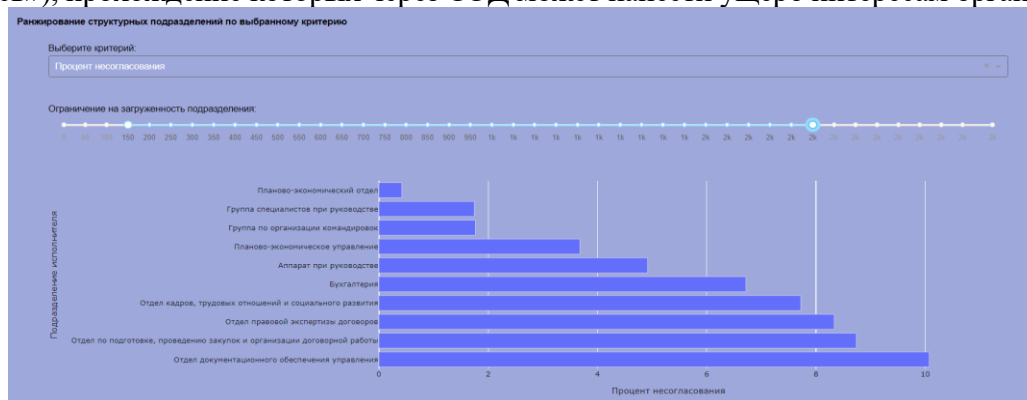


Рис. 8. Ранжирование подразделений по показателю

Fig. 8. Ranking of departments by indicator

Вывод. В представленной публикации рассматривается новая математическая модель СЭД, позволяющая определить численно показатель доступности ЭД с учетом УБИ и выполнять оптимизацию с учетом сложной организационной структуры современных организаций. Предложенная модель обладает новизной: введены новые показатели степени обеспечения ИБ и представлен пример определения доступности при обработке ЭД в конкретной реализации СЭД.

В представленной новой модели могут применять дополнительные показатели обеспечения ИБ, отражающие специфику движения ЭД в корпоративных СЭД. Предложенная модель дополнительно позволяет идентифицировать уязвимости в СЭД, которые могут быть использованы для реализации новых (ранее не документированных) УБИ и содействовать повышению уровня обеспечения ИБ в проектах СЭД.

Библиографический список:

1. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Схемотехнические решения для практической реализации безопасного электронного документооборота. Часть 1. Аналитический обзор. // Газовая промышленность. – 2022. – № 9. – С. 40-56
2. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Схемотехнические решения для практической реализации безопасного электронного документооборота. Часть 2. Новая разработка. // Газовая промышленность. – 2022. – № 11. – С.50-70.
3. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа. Вопросы кибербезопасности. – 2020. - №1 (35). – С. 42 – 51.
4. Круковский М.Ю. Концепция построения моделей композитного документооборота / Математические машины и системы. – 2004. – №2. – С. 149 – 163. EDN: RPCPIH
5. Куприянов Ю.В., Морев С.А. Теоретико-множественная модель системы управления организацией // Алгоритмы, модели и системы обработки данных. – 2006. – №11. – С. 178-183
6. Ланцев Е.А., Доррер М.Г. Агентное имитационное моделирование бизнес-процессов в нотации EEPС//Научно-технический вестник информационных технологий, механики и оптики. 2013. – № 3 (85). – С. 86-92.
7. Елисеев Н.И., Тали Д.И., Обланенко А.А. Оценка уровня защищенности автоматизированных информационных систем юридически значимого электронного документооборота на основе логико-вероятностного метода // Вопросы кибербезопасности. – 2019. – № 6 (34). – С. 7-16. EDN: HIKLQN, DOI: 10.21681/2311-3456-2019-6-07-16

8. Минаев В.А., Королев И.Д., Мазин А.В., Мезенцев А.С., Поддубный М.И. Обоснование формальных систем математической логики для решения задач автоматического электронного документооборота // Радиопромышленность. 2018. № 2. С. 105-114. EDN: XQYSTJ
9. Язов Ю.К. К вопросу об оценке эффективности защиты информации в системах электронного документооборота / Язов Ю.К., Авсентьев О.С., Рубцова И.О. – Вопросы кибербезопасности. – 2019. – №1(29). EDN: YZFWPB, DOI: 10.21681/2311-3456-2019-1-25-34
10. Дровникова И.Г., Алфёров В.П., Овчинникова Е.С. Математическая модель динамики функционирования подсистемы защиты конфиденциальных сведений в системах электронного документооборота // Охрана, безопасность, связь. 2020. № 5-3. С. 175-182. EDN: BKUXCX
11. Краснянский М.Н., Обухов А.Д., Коробова И.Л. Математическая модель обработки информации в системе управления электронным документооборотом//Вестник Тамбовского государственного технического университета. 2018. – Т. 24.–№3.–С.382-399. EDN: YQOAUH DOI: 10.17277/vestnik.2018.03.pp.382-399
12. Вентцель Е.С. Теория вероятностей. Учебник для студентов вузов / Сер. Высшее образование. (9е издание, стереотипное) Москва, 2003.
13. <https://www.securitylab.ru/news/530833.php>
14. <https://www.securitylab.ru/news/537510.php>

References:

1. Livshits I.I., Sokolov E.O., Lukyanova A.A. Circuit solutions for the practical implementation of secure electronic document management. Part 1. Analytical review. *Gas industry*. 2022; 9.: 40-56 (In Russ)
2. Livshits I.I., Sokolov E.O., Lukyanova A.A. Circuit solutions for the practical implementation of secure electronic document management. Part 2. New development. *Gas industry*. 2022; 11: 50-70. (In Russ)
3. Livshits I.I. Cyber risk management practice in oil and gas projects of holding-type companies. *Cybersecurity issues*. 2020; 1 (35): 42 – 51. (In Russ)
4. Krukovsky M.Yu. Concept of constructing composite document flow models. *Mathematical machines and systems*. 2004;2:149 – 163. EDN: RPCPIH (In Russ)
5. Kupriyanov Yu.V., Morev S.A. Set-theoretical model of the organization management system. *Algorithms, models and data processing systems*. 2006;11: 178-183 (In Russ)
6. Lancev E.A., Dorrer M.G. Agent-based simulation modeling of business processes in the EEPС notation. *Scientific and technical bulletin of information technologies, mechanics and optics*. 2013; 3 (85): 86-92.
7. Eliseev N.I., Tali D.I., Oblanenko A.A. Assessment of the security level of automated information systems of legally significant electronic document management based on the logical-probabilistic method. *Cybersecurity Issues*. 2019; 6 (34): 7-16. EDN: HIKLQN, DOI: 10.21681/2311-3456-2019-6-07-16 (In Russ)
8. Minaev V.A., Korolev I.D., Mazin A.V., Mezentsev A.S., Poddubny M.I. Justification of formal systems of mathematical logic for solving problems of automatic electronic document management. *Radio industry*. 2018; 2:105-114. EDN: XQYSTJ (In Russ)
9. Yazov Yu.K. On the issue of assessing the effectiveness of information protection in electronic document management systems / Yazov Yu.K., Avsentyev O.S., Rubtsova I.O. *Cybersecurity Issues*. 2019;1 (29). EDN: YZFWPB, DOI: 10.21681 / 2311-3456-2019-1-25-34 (In Russ)
10. Drovnikova I.G., Alferov V.P., Ovchinnikova E.S. Mathematical model of the dynamics of the functioning of the subsystem for the protection of confidential information in electronic document management systems. *Security, Safety, Communications*. 2020; 5-3:175-182. EDN: BKUXCX (In Russ)
11. Krasnyansky M.N., Obukhov A.D., Korobova I.L. Mathematical model of information processing in the electronic document management system. *Bulletin of Tambov State Technical University*. 2018; 24(3):. 382-399. EDN: YQOAUH DOI: 10.17277/vestnik.2018;03:382-399 (In Russ)
12. Ventzel E.S. Probability Theory. Textbook for University Students / Series: Higher Education. (9th edition, stereotyped) Moscow, 2003. (In Russ)
13. <https://www.securitylab.ru/news/530833.php>
14. <https://www.securitylab.ru/news/537510.php>

Сведения об авторе:

Лившиц Илья Иосифович, доктор технических наук, профессор практики, Livshitz.i@yandex.ru

Information about author:

Ilya I. Livshits, Dr. Sci.(Eng.), Prof. of Practice; Livshitz.i@yandex.ru

Конфликт интересов/Conflict of interest.

Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.

Поступила в редакцию/ Received 18.06. 2024.

Одобрена после рецензирования/ Reviced 22.07.2024.

Принята в печать/ Accepted for publication 12.10.2024.