

**ЧИСЛЕННАЯ ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КОМПАНИИ
ХОЛДИНГОВОГО ТИПА**

Шеховцова И.Р. (Университет ИТМО)

Научный руководитель – профессор, доктор технических наук Лившиц И.И.
(Университет ИТМО)

Введение. Известно, что многие крупные компании (например: ПАО «Сбербанк», ПАО «Газпром нефть», ПАО «Ростелеком» и иные) реализуют программы в области цифровой трансформации и импортозамещению, в том числе, инициативы по внедрению различных систем электронного документооборота (далее – СЭД) [1, 2]. Создание современных надежных и безопасных систем СЭД требует обработки значительного количества документов в цифровом виде. В то же время из-за несовершенства процессов достоверных управляемых информационных потоков возможны ситуации, при которых некоторая часть электронных документов может не быть обработана должным образом в ожидаемое время. Соответственно, нарушения обработки ЭД могут привести к существенным потерям для компании, и этот негативный эффект будет еще более значительным в корпоративных информационных системах компаний холдингового типа [3].

Основная часть. В современных СЭД определенный электронный документ недоступен пользователю, пока не поступит конкретная задача его обработки. При наличии отклонений в маршруте электронного документа, в т.ч. временных, документ может не достигнуть своего адресата в заданное время. В связи с этим в СЭД может нарушаться доступность информации – важное свойство ИБ, определяющее возможность использования объекта субъектом по запросу (например, в соответствии с требованиями известных стандартов ГОСТ Р ИСО/МЭК 27001-2021, ISO/IEC 27001:2022). Соответственно, из указанного положения логично следуют требования к безопасности и надежности, предъявляемые к такому объекту, как СЭД. Для СЭД предлагается ввести такие критерии безопасности, как гарантирование достижения финала маршрута и общая безопасность корпоративной информационной системы. Безопасная СЭД должна не только автоматизировать движение документов, но и обеспечивать эффективность с точки зрения выбранного критерия (критериев) по маршрутам. В этом аспекте представляется обоснованным внимание к оптимизационным задачам, связанным с нахождением оптимальных путей прохождения (маршрутов) электронных документов в СЭД и гарантирующих успешное достижение финальных точек.

При рассмотрении бизнес-процессов в СЭД разумно представлять процессы движения электронных документов таким образом, что переходы объектов (документов) из состояния в состояние происходят под действием потоков событий. Автором предлагается модель электронного документооборота, описанная в рамках теории дискретных марковских случайных процессов с непрерывным временем.

Построенная модель позволяет перейти к важной и актуальной задаче – формированию численной оценки рисков информационной безопасности в СЭД (например, в соответствии с требованиями ГОСТ Р ИСО 31000–2019 или ISO 31000:2018). В рамках исследуемой задачи под риском понимается оценка негативных последствий отклонения от запланированных переходов по фиксированному маршруту. Каждому состоянию процесса обработки конкретного электронного документа можно сопоставить некоторую оценку – доход, обеспечиваемый единицей моделируемой системы (СЭД) или приходящиеся на нее потери, связанные с несвоевременной подготовкой документа, задержками в согласовании, ошибками в заполнении или некомпетентностью персонала. 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.

Заключение. Предложена новая математическая модель для оценки безопасности СЭД с учетом угроз безопасности информации для электронных документов, обрабатываемых в корпоративной информационной системе нефтегазовой компании холдингового типа. Модель позволяет определять эффективность комплекса действующих мер защиты электронных документов от конкретных угроз безопасности информации и количественно обосновывать требования ко времени обработки документа. Предложенная модель дополнительно позволяет идентифицировать уязвимости в СЭД, которые могут быть использованы для реализации новых (ранее не документированных) угроз безопасности информации.

Список использованных источников:

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.