Бородин Андрей Викторович
канд. экон. наук, доцент, заведующий кафедрой
Никитин Радик Юрьевич
магистрант
Ширяев Андрей Игоревич
магистрант
ФГБОУ ВО «Поволжский государственный технологический университет»
г. Йошкар-Ола, Республика Марий Эл

DOI 10.21661/r-114000

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ И ПОДЛИННОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИИ НА БУМАЖНОМ НОСИТЕЛЕ ПРИ ОТЧУЖДЕННОЙ ОБРАБОТКЕ ДОКУМЕНТА

***Аннотация**: в данной работе авторами предложен механизм обеспечения целостности документа при переносе процессов печати и подписания документа на бумажном носителе на сторону клиента в условиях, когда процессы на стороне клиента не подконтрольны контрагенту.*

***Ключевые слова**: документ, модель угроз, онтологическая модель, политика безопасности, целостность, электронная цифровая подпись, юридическая сила, QR-код.*

Сегодня технологии электронной цифровой подписи (ЭЦП) распространены во всех сферах бизнеса и востребованы в основном юридическими лицами. Постепенно они внедряются и в практическую деятельность физических лиц. При наличии ЭЦП для физического лица открывается ряд новых и интересных возможностей:

1) быстрый доступ к полному объему сервисов Единого портала государственных услуг;

2) дистанционная подача заявления на поступление в высшее учебное заведение;

3) участие в электронных торгах на поставку товаров и оказание услуг;

4) регистрация юридического лица или индивидуального предпринимателя;

5) быстрое дистанционное оформление заявки на получение патента на изобретение.

Этот список постоянно расширяется.

Однако использование ЭЦП требует от физического лица наличия определенной технической культуры и понимания основных принципов обеспечения безопасности в области информационных технологий. С другой стороны, если посмотреть на перечень субъектов обеспечения этих новых возможностей, то там оказываются в основном государственные структуры или организации аффилированные с этими структурами, что связано, в частности, с особенностями правоприменения закона «Об электронной подписи».

В этих условиях организации, чья экономическая деятельность связана с сетью Internet и которым требуется наличие механизма признания юридической силы соглашений (документов), подписанных контрагентами – физическими лицами, вынуждены использовать суррогатные технологии дистанционной подписи документов. Одной из таких технологий является подход, основанный на отправке клиенту соглашения об оказании услуг по каналам сети Internet с последующей распечаткой документа на стороне клиента, собственноручным подписанием соглашения клиентом и отправкой подписанного документа традиционной почтой. При этом получение организацией файла, содержащего скан подписанного документа, может означать возможность оказания услуги клиенту в ограниченной форме. Получение подлинника по почте обеспечивает полномасштабное оказание услуги, являющейся предметом подписанного соглашения. Второй экземпляр бумажного подлинника после физического подписания ответственным сотрудником и заверения печатью может быть направлен обратно почтовым отправлением клиенту. Такая возможность может быть связана с необходимостью повышения доверия клиента к организации.

Описанная суррогатная технология несет определенные угрозы для организации, взаимодействующей таким образом со своими клиентами. В частности,

подписываемое соглашение может содержать индивидуальные, существенные для клиента, условия, которые он может изменить в одностороннем порядке при переносе направленного ему по каналам Internet документа на бумажный носитель. В последствии, клиент может попытаться, ссылаясь на подписанный документ, оспаривать условия оказания ему услуг со стороны организации. При допущении возможной невнимательности ответственного сотрудника при реализации механизма возврата клиенту подписанного и заверенного печатью организации второго экземпляра подлинника описанная угроза может стать юридически существенной.

В настоящей статье представлен онтологический анализ описанной ситуации, базирующийся на методологии, разработанной автором [1; 3; 7], и использующий нотацию IDEF5 [2]. На основе проведенного анализа предложены основные технические решения, составляющие базу для синтеза соответствующей политики безопасности.

Онтологическая модель описанной проблемы представлена на рис. 1. Словари элементарных угроз и противодействий приведены, соответственно, в таблицах 1 и 2.

Таблица 1

Словарь элементарных угроз

Угроза	*Описание угрозы*
U_0	Использование контрагентом (клиентом) документа с несанкционировано модифицированной критической частью. (Документ, при этом, ошибочно прошел процедуру проверки и подтверждения.)
U_1	Несанкционированная модификация критической части документа со стороны и на стороне контрагента (клиента) во время подготовки документа к печати
U_2	Несанкционированная модификация контрольной информации с целью атаки на содержание критической части документа
U_3	Атака на аутентичность документа на основе повторного использования образца жесткой связи «критическая часть документа» – «контрольная информация»
U_4	Низкая надежность канала «электронный документ – печать – бумажный экземпляр – сканирование» для контрольной информации

Таблица 2

Словарь элементарных противодействий атакам

Противо-действие	*Описание противодействия*
P_1	Контроль целостности критической части документа на основе контрольной информации, внедренной в документ. (При этом для контрольной информации доступен процесс переноса на бумажный носитель при печати.)
P_2	Использование для защиты жесткой связи «критическая часть документа» – «контрольная информация» механизма электронной цифровой подписи
P_3	Использование при формировании контрольной информации случайного идентификатора события, даты и времени согласования, а также информации об ответственном сотруднике, согласовавшем содержание критической части документа
P_4	Использование QR-кодов для переноса контрольной информации
P_5	Декларация об аутентичности документа лишь при условии сохранения возможности считывания QR-кода. (Декларация должна быть включена в текстовую часть документа.)
P_6	Подтверждение организацией юридической силы документа при условиях успешного считывания QR-кода и подтверждения целостности критической части документа

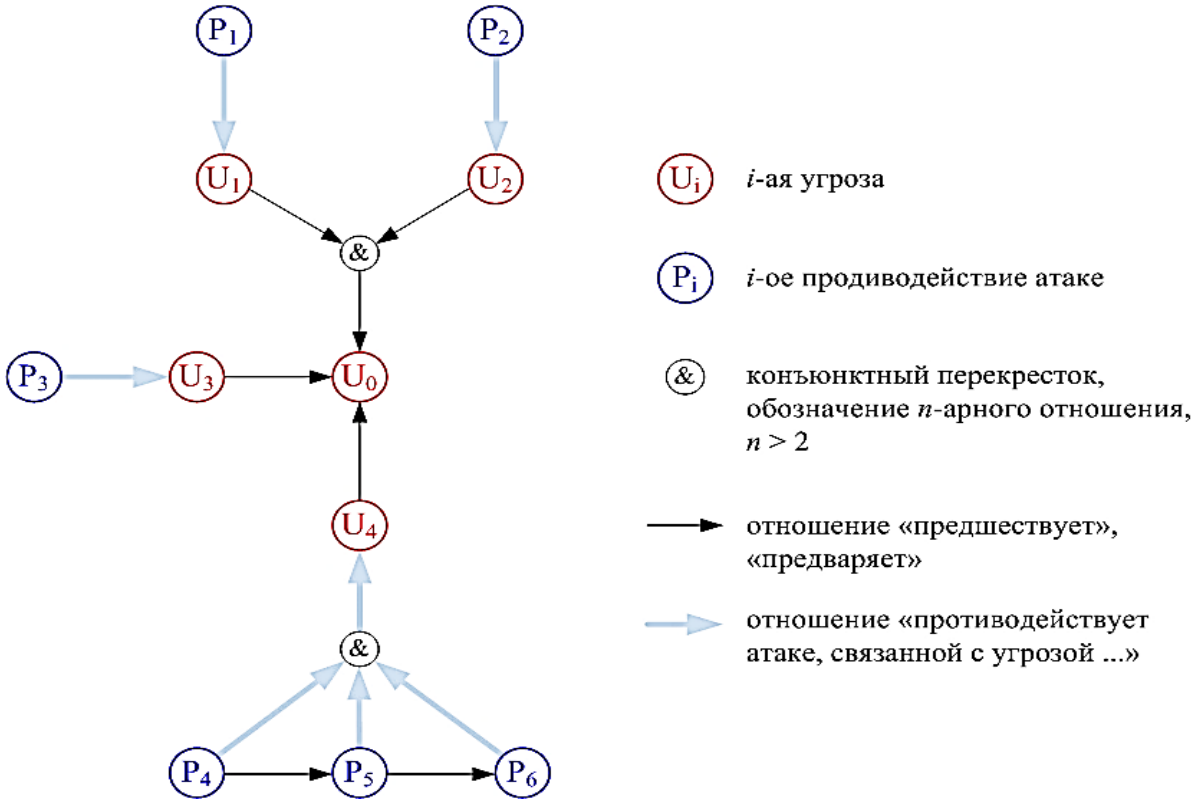

Рис. 1. Онтологическая модель реализации политики безопасности для процессов отчужденной обработки информации

Проведенный онтологический анализ позволяет сформулировать основные этапы защищенной обработки документа, подвергаемого отчужденной обработке:

1. Согласование организацией содержания документа с клиентом. Формирование уникального идентификатора сделки. Фиксация времени сделки.

2. Выделение критической части документа. Критическая часть документа должна включать в себя уникальный идентификатор и время совершения сделки. Наличие в документе уникального идентификатора и времени совершения сделки обеспечат взаимно однозначное соответствие бумажного оригинала документа и его электронной копии (электронных копий) [6].

3. Формирование ЭЦП критической части документа с использованием секретного ключа ответственного за сделку сотрудника организации.

4. Внесение ЭЦП критической части документа в документ в формате QR-кода [5], а также включение в текстовую часть документа декларации об аутентичности документа лишь при условии сохранения возможности считывания QR-кода.

5. Отправка документа клиенту в электронном виде по каналам сети Internet.

6. Отчужденная обработка документа, включающая в себя печать документа на стороне клиента, его подписание клиентом и отправку бумажного оригинала организации с использованием традиционной почтовой связи.

7. Получение оригинала документа организацией. Двухэтапная проверка аутентичности документа на основе скана: визуальный контроль при наложении скана на исходное графическое изображение документа и автоматизированный контроль на основе распознавания QR-кода и проверки сохранности ЭЦП.

8. В случае успешной проверки, подтверждение юридической силы документа подписью ответственного сотрудника и печатью.

9. Отправка бумажного оригинала клиенту с использованием традиционной почтовой связи.

Структурная модель документа, соответствующая предложенной политике безопасности, приведена на рис. 2. Здесь использованы следующие обозначения:

m – исходный текст документа;

Substr – функция, выделяющая из текста заданную часть;

m_0 – некритическая часть текста документа;

m_1 – критическая часть текста документа;

h – криптографическая хеш-функция;

DS – функция, реализующая асимметричное криптографическое преобразование;

$k_i^{(priv)}$ – секретный ключ i-го ответственного сотрудника компании;

QR – функция, формирующая QR-код своего аргумента.

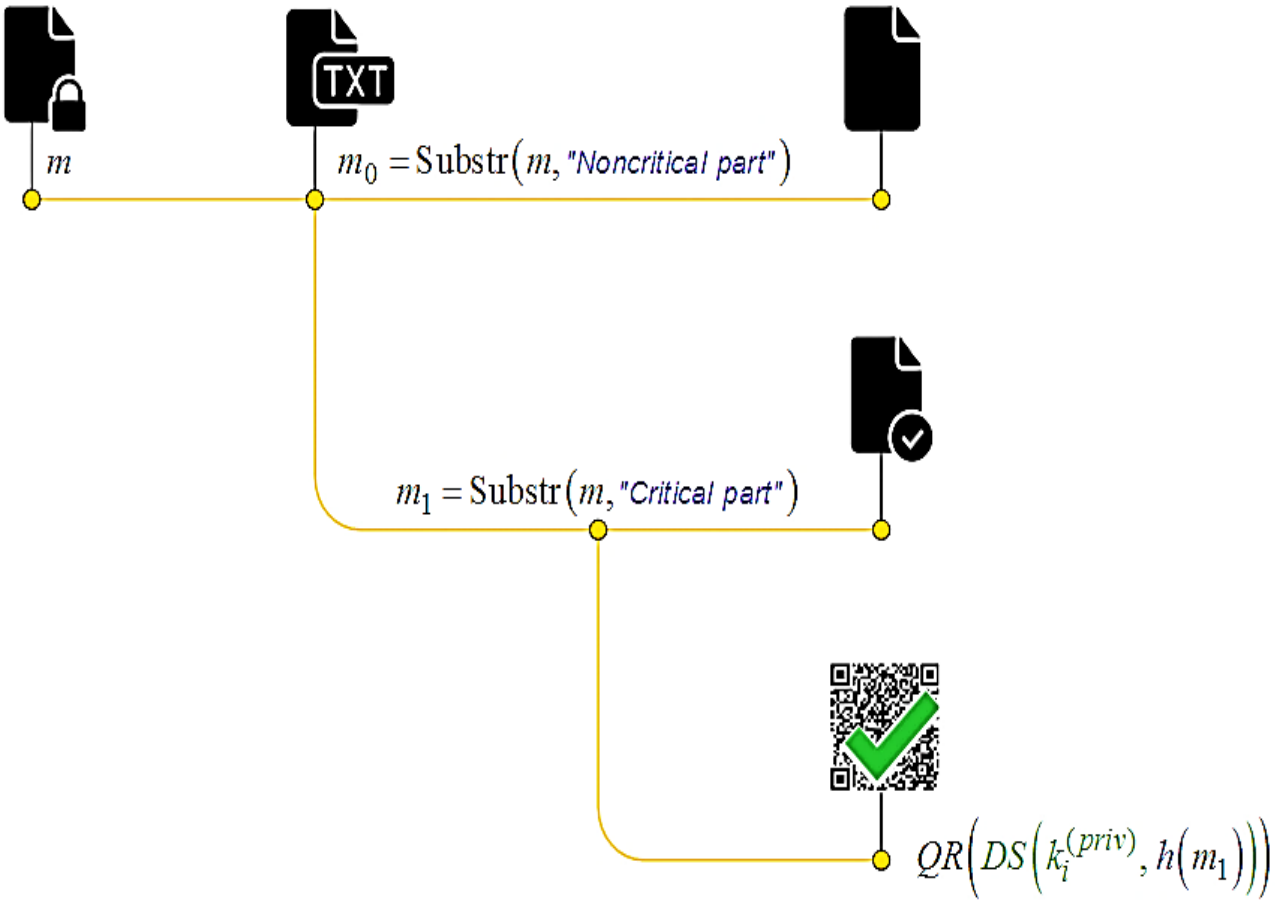

Рис. 2. Структурная модель документа

Предложенная политика безопасности, а также механизмы формирования электронного документа (для переноса на бумажный носитель и подписания бумажной версии документа на стороне клиента) и последующей проверки бумажного документа организацией были апробированы на базе расширения функциональности экспериментальной системы электронного документооборота [4]. В дальнейшем данная разработка предполагается к использованию в подсистеме розничных платежей одного из российских операторов по переводу денежных средств клиентов.

Список литературы

1. Бородин А.В. Методологические основы моделирования в задачах экономики безопасности / А.В. Бородин // Современные проблемы и перспективы социально-экономического развития предприятий, отраслей, регионов. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – С. 217–222.

2. Бородин А.В. Метод онтологического анализа IDEF5 в задачах структурного синтеза динамических моделей угроз / А. В. Бородин // Обозрение прикладной и промышленной математики. – 2006. – Т. 13. – В. 3. – С. 474–475.

3. Бородин А.В. Онтологические модели в экономике безопасности / А.В. Бородин // Труды Поволжского государственного технологического университета. Серия: Социально-экономическая. Вып. 2. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – С. 14–19.

4. Бородин А.В. Открытая система визуального документооборота со встроенной поддержкой электронной цифровой подписи / А.В. Бородин // Труды Марийского государственного технического университета. Вып. 2: Материалы научной конференции профессорско-преподавательского состава, докторантов, аспирантов, сотрудников Марийского государственного технического университета (27–31 мая 1996 г.). Ч. III. – Йошкар-Ола: Марийский государственный технический университет, 1996. – С. 20–22.

5. Бугаев Л. Мобильный маркетинг: Как зарядить свой бизнес в мобильном мире / Л. Бугаев. – М.: Альпина Паблишер, 2012. – 214 с.

6. Конявский В.А. Основы понимания феномена электронного обмена информацией / В.А. Конявский, В.А. Гадасин. – Минск: Беллитфонд, 2004. – 282 с.

7. Borodin A.V. System of instrumental and mathematical methods of the solution of task of economy of safety / A.V. Borodin // Global Science and Innovation: materials of the III International Scientific Conference (Chicago, October 23–24th, 2014). – Chicago: Publishing office Accent Graphics communications, 2014. – P. 314–317.