ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ СЕРВИСОВ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПРЕДПРИЯТИЯ

Л.Н. Иванова, А.В. Киреева (Санкт-Петербург)

На сегодняшний день значительное количество предприятий прибегают к внедрению и впоследствии к использованию электронного документооборота (ЭДО) в связи с необходимостью упрощения и автоматизации цикла работы с документами, что положительно воздействует на решение управленческих задач.

В большинстве случаев платформа автоматизации документооборота становится чрезвычайно необходимой при реализации современных концепций управления бизнес процессами, такими, как сопровождение документов, менеджмент знаний, управление качеством при исполнении договоров. Помимо этого, оптимизированные системы документооборота предоставляют возможность ускоренного режима выполнения поставленных задач и позволяют опередить конкурентов в принятии оперативно-стратегических решений.

Основными принципами ЭДО являются [1]:

1) однократная регистрация документа;

2) возможность параллельного выполнения различных операций с целью сокращения времени движения документов и повышения оперативности их исполнения;

3) единая база для централизованного хранения информации;

4) эффективно организованная система поиска документов;

5) развитая система отчётности по различным статусам и атрибутам документов, позволяющая контролировать движение документов.

Многие предприятия опасаются предпринимать необдуманные шаги по внедрению систем автоматизированного ЭДО в связи с существованием определенного ряда рисков, к которым можно отнести [2]:

1) административные риски: недостаточное внимание высшего руководства к проекту, загруженность занятых сотрудников и их слабая вовлеченность в проект;

2) организационные риски: недостаточное планирование, отсутствие или некорректная постановка целей и задач проекта, несогласованность действий в процессе выполнения задач, отсутствие или неэффективное управление коммуникациями внутри проекта;

3) субъективные риски: отсутствие навыков работы с компьютером, недостаточный опыт работы с информацией в электронном виде, резкое сопротивление нововведениям со стороны сотрудников и руководства предприятия;

4) технологические риски: неготовность ИТ-инфраструктуры, недостаточное исследование потребностей предприятия и отсутствие нормативной базы.

Недооценка важности этапа учета рисков может существенно замедлить разработку и реализацию проекта, вдобавок серьезно повлияет на ожидаемый результат. Более того, работа над проектом может быть остановлена на неопределенный срок, в результате чего предприятие вероятнее всего понесет убытки.

В зависимости от технологий хранения информации существует множество методов работы с электронными документами. Облачные технологии, представляющие собой один из таких методов, набирают все большую популярность и имеют весьма привлекательные перспективы развития. Именно по этой причине защита информации, которая хранится в облаке, как никогда актуальна.

В России активно используются облачные вычисления 1С: Предприятия, обеспечивающие повсеместную работу на разных клиентских устройствах с

различными операционными системами. В этой системе облачные технологии могут использоваться как отдельным клиентом, так и внутри организации и холдинга, объединяющего несколько компаний. Сотрудники имеют возможность подключаться к информационной базе из любых мест. Вместе с тем, в холдинге сокращаются расходы на администрирование одинаковых прикладных решений, и может осуществляться синхронизированное обновления [3].

К основным преимуществам применения облачных технологий в ЭДО можно отнести:

1) доступность информации, позволяющая сотрудникам становиться более мобильными;

2) экономия денежных средств на приобретение, установку и поддержку соответствующего программного обеспечения (ПО);

3) сокращение времени поиска нужной информации при централизованном хранении данных;

4) облегчение процесса сотрудничества с другими предприятиями путем безопасного просмотра, обмена информацией через облачную платформу;

5) удобство использования, содействующее повышению производительности труда сотрудников, которые меньше отвлекаются от текущих задач;

6) повышенная отказоустойчивость и безопасность;

7) масштабируемость облачного сервиса в короткие сроки по мере необходимости.

Большинство предприятий по данным на октябрь 2020 года активно используют облачные технологии – 66% находятся на продвинутой или промежуточной стадии внедрения облачных технологий (рис. 1) [4].

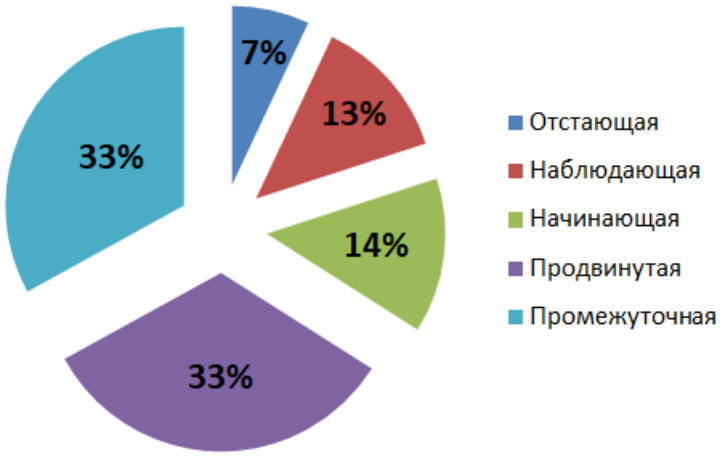

Рисунок 1 – Стадии внедрения облачных технологий

Стадии внедрения:

1) отстающая – облачные технологии не применяются, и нет планов по их внедрению;

2) наблюдающая – стратегия использования облачных процессов в разработке, сами технологии не применяются;

3) начинающая – облачные технологии в процессе внедрения или уже внедрены и реализованы для одного проекта, как минимум;

4) продвинутая – облачные технологии задействованы для значительной части ИТ-инфраструктуры или процессов;

5) промежуточная – облачные технологии используются для поддержания одного или нескольких процессов/систем; в планах расширение области применения облачных технологий.

Объем российского рынка публичных облачных сервисов в 2019 году составил 73 млрд. руб., что на 30% больше показателя годичной давности. Об этом свидетельствуют данные аналитического агентства «ТМТ Консалтинг» (рис. 2) [5]. В IDC Russia одним из важнейших стимулов роста российского рынка облачных услуг называют растущую популярность аналитики больших данных для решения бизнес-задач, получения конкурентного преимущества и управления рисками [6].

Рисунок 2 – Объем и динамика рынка публичных облачных услуг в России в 2016-2024 г., млрд. руб.

Обратимся к практическому опыту применения информационно-коммуникационных технологий в промышленности. Некоторые судостроительные предприятия (например, – Lampell, занимающееся производством нефтяных платформ) уже сейчас применяют облачную технологию SSI Enterprise Platform, которая позволяет в удобном виде реализовать интеграцию информации, т.е. организовывать процесс переноса данных из одного источника в другой.

Автоматизируя и анализируя процессы управления, предприятие экономит немалые средства при использовании этой системы. На основе электронной обработки информации ведется работа сварочных роботов, управление строительством и станков с ЧПУ. Данные из облака доступны не только инженерным и производственным отделам, но и службам логистики, качества, безопасности, финансовым службам. Такой подход к использованию ЭДО является экономически эффективным [7].

Информационные технологии внедряются в управление жизненным циклом продукции. В связи с увеличением спроса на многоцелевые суда, оснащенные новыми видами оборудования, повышается неопределенность при постройке. Эта неопределенность связана с увеличением числа бортовых систем, что усложняет проверку правильности процессов сборки, также габариты, технические характеристики и даже цены на новое оборудование на начальном этапе точно неизвестны. Если вносить изменения в конструкцию на поздних этапах производственного цикла, то это приведет к нарушению процессов конструирования и постройки судна, что ведет к дорогостоящим задержкам по времени. Виртуальное моделирование производственного процесса строительства судна позволит легко и просто при внесении изменений пересчитать сроки и степень загрузки производственных мощностей. Для этого в информационную модель судна нужно внести параметр времени. Эта концепция получила название 4D-Planning. Она

напрямую связана с облачным ЭДО (известны такие CAPP-системы, как Tecnomatrix и Teamcenter производства Siemens PLM Software), где учитывается фактор времени, позволяя создавать реалистичные планы строительства судна и даже прогнозировать риски при возможном изменении последовательности сборки корабля. Такие системы могут быть развернуты как локально (on-premise), так и в облаке. Эти системы могут заранее запрограммировать сварочные роботы, чтобы те приступили к сварке стальных узлов, когда узлы появятся на строительной площадке [7].

Невзирая на то, что трехмерное, а в некоторых случаях и четырехмерное проектирование стало стандартом фактически на всех судостроительных предприятиях, в российской судостроительной отрасли все еще нет единого понимания «информационной модели судна», которое позволит в дальнейшем создавать «виртуальные предприятия» [7].

При всех, безусловно, положительных аспектах применения облачных технологий, необходимо рассмотреть главные угрозы безопасности в облаке и методы защиты:

1) Недостаточный уровень информационной безопасности провайдера. В данном случае внутренние требования безопасности используемого облачного сервиса не согласованы, другими словами, нет поддержки необходимого уровня контроля защиты. Перед тем как выбрать облачного провайдера нужно провести анализ предоставляемых им облачных сервисов с учетом цели использования облака и чувствительной информации, которая будет обрабатываться. Также в обязательном порядке требуется ознакомиться с сертификацией провайдера, условиями соглашения об оказании услуг, определяющих общие меры защиты и обязанности клиента и провайдера, в том числе отслеживать обновления соглашений, которые в дальнейшем могут отразиться не самым благоприятным образом на безопасности информационных ресурсов предприятия. Важно ознакомиться с тем, каким образом поставщик облачного хранилища использует шифрование внутри облака и при передаче данных между центрами обработки данных, серверами и устройствами.

2) Неконтролируемый доступ к облачным сервисам включает такие проблемы как получение доступа с не доверенных и уязвимых устройств, отсутствие контроля данных, передаваемых во внешние сервисы, а также имеющие доступ к информации бывшие сотрудники. Основными средствами нейтрализации данной угрозы являются разработка политики разграничения доступа к ресурсам и регламента контроля доступа пользователей к облачным сервисам, включающего комплекс организационных и технических мер, регулярное проведение аудита и тестирования на проникновение. Кроме того, для обеспечения безопасности следует проверять журналы доступа, чтобы убедиться в том, что только авторизованные сотрудники имеют доступ к конфиденциальным данным в облаке. К тому же допускается широкое использование многофакторной аутентификации на всех устройствах и системах, снижающее риск получения доступа к системе с целью хищения ценной информации.

3) Перехват контроля ресурсов. При появлении какого-либо незащищённого сервиса, злоумышленнику не составит труда им воспользоваться. Причиной чаще всего является отсутствие единой структурированной политики безопасности и удобных инструментов контроля вносимых изменений. В таких случаях надлежит постоянно отслеживать состояние ресурсов в облаке и разработать политику безопасности облачных активов.

4) Несанкционированный доступ к API. Проблемы в области информационной безопасности, касающиеся отсутствия разграничения и контроля доступа к API, внедрения вредоносного кода в запросы API, эксплуатации уязвимостей аутентификации и авторизации API приводят к реализации данной угрозы. Для

устранения опасности необходимо проводить тестирования на проникновение, разработать требования к управлению доступом к API, спроектировать и внедрить межсетевой экран для веб-приложений.

5) Утечка конфиденциальных данных. Дабы не допустить утечку информации нужно осуществлять контроль данных при передаче, хранении и обработке, используя защищенные каналы и шифрование.

6) Использование Shadow IT. Под Shadow IT понимаются электронные устройства, сервисы и ПО, которые находятся на предприятии, но не обслуживаются ИТ-отделом, т.е. их состояние и работа не контролируются. Решением в данном случае может послужить использование различных инструментов для выявления и ограничения подключений к используемым сервисам.

Таким образом, подводя итоги, отметим, что следуя предложенным рекомендациям по обеспечению защиты электронных документов в облачном сервисе, предприятия могут снизить риски прогнозируемых угроз.

Литература

1. Электронный документооборот (общее делопроизводство) [Электронный ресурс]. Режим доступа: http://www.viaduk.net/docflow.
2. Внедрение системы электронного документооборота: риски и способы их преодоления [Электронный ресурс]. Режим доступа: https://www.tadviser.ru/a/160193.
3. Материалы XIX Международной научно-практической конференции «Документация в информационном обществе: «облачные» технологии и электронный документооборот», 24-25 октября 2012 г. Москва, ВНИИДАД.
4. Исследование PwC «Страх облаков» [Электронный ресурс]. Режим доступа: https://www.pwc.ru/ru/publications/pwc-cloud-fear-survey.pdf.
5. Рост российского рынка публичных облаков на 30% - TMT Консалтинг [Электронный ресурс]. Режим доступа: https://www.tadviser.ru/a/109894.
6. Рынок облачных услуг России перевалил за миллиард долларов [Электронный ресурс]. Режим доступа: https://www.cnews.ru/news/top/2020-10-20_rynok_oblachnyh_uslug_rossii.
7. Облачные технологии в судостроении [Электронный ресурс]. Режим доступа: https://www.it-grad.ru/blog/oblachnye-texnologii-v-sudostroenii.