



Рис. 2. Преимущества использования облачных решений по мнению финансовых директоров [2]

Не смотря на множество преимуществ облачные технологии обладают рядом недостатков:

- Отсутствие доступа к внутренней инфраструктуре облака из-за того, что пользователи не являются его владельцами;
- Безопасность личной информации в значительной степени зависит от компании-провайдера;
- Возможности использования ограничиваются скоростью сети Интернет;
- Большая роль человеческого фактора в ошибках системы.

Для малого бизнеса, не имеющего финансовых ресурсов для приобретения программного обеспечения, а также организационной инфраструктуры, необходимой для его использования, облачные сервисы являются хорошей возможностью сберечь средства [2].

В январе 2017 г. Oracle представила исследование, проведенное по ее заказу в России, чтобы выявить взгляд финансовых директоров на облачные сервисы. Исследование показало, что каждая третья компания ищет новые стратегические подходы к развитию бизнеса и более эффективные ИТ-решения. 75% опрошенных руководителей указали снижение издержек компании как один из важнейших приоритетов в стратегии на ближайшие три года, 33% – замену ИТ-решений и поиск малозатратных альтернатив (рис. 2).

Анализируя поставленную задачу, нами были выявлены особенности применения облачных технологий. Так, система программ «1С: Предприятия» создает все условия для универсальной и благоприятной работы с всевозможными решениями на любом клиентском оборудовании. Заказчики могут даже не устанавливать систему программ компании на свое оборудование, либо устанавливать простое и компактное клиентское приложение.

При использовании облачных технологий компании платят только за их аренду. Возможность работы с системой зависит только от наличия доступа в сеть Интернет, а ответственность

за обслуживание и обновление системы несет служба технической поддержки поставщика. Таким образом, облачные технологии позволяют сэкономить на приобретении, поддержке, совершенствовании программного обеспечения и оборудования [2].

Прогресс облачных технологий дал важнейший толчок для распространения проектного менеджмента в малом и среднем бизнесе России. Затраты на создание информационной инфраструктуры свелись к минимуму, а программирование систем управления проектами в стандартном web-интерфейсе позволило сократить расходы на обучение персонала.

В настоящее время в информационной среде первостепенную роль играют облачные технологии, что демонстрирует тенденцию ближайшего будущего о появлении простых и удобных систем управления проектами практически во всех сферах бизнеса.

#### Список литературы

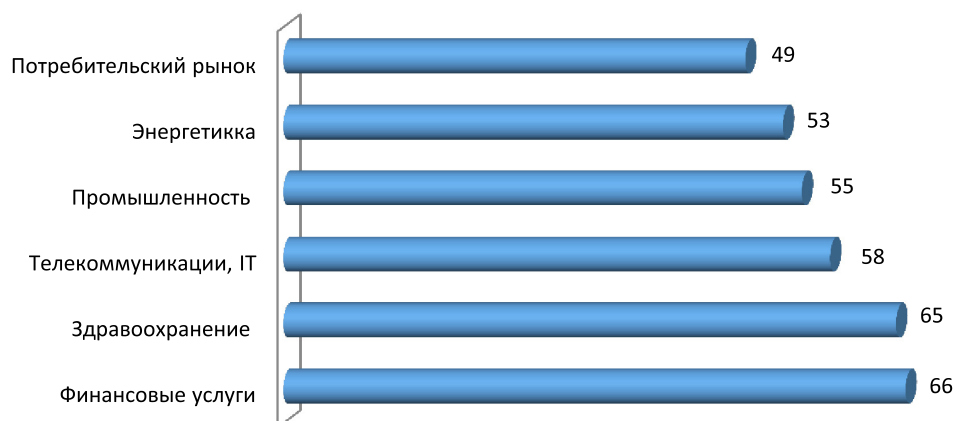
1. Захаров Д.К. Облачные технологии в системе управления персоналом // Вестник университета. 2016. № 5. С. 190-196.
2. Ли Е.А., Трофимова Л.А., Перова М.А. Современные технологии в цифровой экономике. Как построить и развить свой он-лайн бизнес в интернете // Научное обозрение. Педагогические науки. 2019. № 2-2. С. 72-74.

#### ЦИФРОВАЯ СРЕДА ДОВЕРИЯ

Апроян А.А., Шевкунова М.А.

*Южно-Российский институт управления филиал  
Российской академии народного хозяйства  
и государственной службы при Президенте РФ,  
e-mail: Aproyan97@bk.ru*

Актуальность данной темы обусловлена тем, что в настоящее время процесс цифровизации затрагивает практически все сферы жизнедеятельности и поэтому вопрос доверия к электронным документам является важным. Результатом исследования является определение путей повышения уровня доверия граждан к цифровой среде.



*Степень превентивности по управлению рисками, % [2]*

В настоящее время в Российской Федерации одним из приоритетных направлений государства является построение цифровой экономики в стране для повышения ее конкурентоспособности, улучшения качества жизни граждан, обеспечения экономического роста. Роль электронного документооборота стремительно возрастает в связи с тем, что информация, предоставленная в цифровом виде, это ключевой фактор производства в социально – экономической сфере деятельности. В соответствии с Указом Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в РФ 2017 – 2030» был обозначен ряд приоритетных задач, направленных на формирование доверия к электронным документам [1].

По мнению экспертов информационная среда значительно изменилась и большее значение придается цифровым рискам, а не информационной безопасности. Актуальность подобных рисков на российском рынке очевидна из – за возникающих вопросов кибербезопасности и защиты персональных данных, которые стали взаимосвязаны.

Все компании, реализующие проект цифровой трансформации на своем предприятии, стараются применять новые технологии для решения многих проблем и ускорения темпов развития. По данным международной сети компаний PricewaterhouseCoopers (PwC) 53% респондентов во всем мире с самого начала работы считает предупредительные меры по управлению рисками необходимой частью любого проекта, в то время как в России этот показатель равен 30%.

Приведенная ниже статистика по управлению рисками в сферах услуг варьируется в зависимости от выбранной индустрии (рисунок).

Одной из возможностей снижения рисков и решения задач, связанных с нарушением информационной безопасности и конфиденциаль-

ности персональных данных является повышение квалификации сотрудников и руководства. В иностранных компаниях 39% сотрудников уверены в том, что ответственность за кибербезопасность и защите данных (40%) закреплена за их руководителем, а в России это процентное соотношение 24% и 21% соответственно. Каждый сотрудник организации должен быть осведомлен в вопросах защиты своих данных. И лишь у 34% участников опроса внедрена система осведомленности.

Для обеспечения киберустойчивости требуется гибкость как в плане обороны, так и восстановления. Устойчивые к внешним воздействиям системы позволяют компаниям в момент кибератаки не прерывать по возможности свою деятельность и быстро восстанавливаться в случае сбоев. Это жизненно важно для компаний, потому что нарушение или приостановка деятельности могут сразу же привести к финансовым потерям, которые зачастую превышают убытки от незащищенности данных и нарастают гораздо быстрее. Когда же компании начнут принимать больше решений на основе данных при помощи искусственного интеллекта, задача сохранения целостности данных станет еще актуальнее.

Всего около половины средних и крупных компаний в основных секторах экономики утверждают, что ведут активную работу по повышению своей устойчивости к кибератакам и другим дестабилизирующим событиям. Но в том, что их компания соответствующим образом проверила свою устойчивость к кибератакам, уверены менее половины из них.

В процессе международной научно – практической конференции «Единая цифровая среда доверия – правовые аспекты» экспертами были выявлены проблемы в области соблюдения законодательных стандартов и требований, принципов в цифровой сфере и этических норм,

которые сводятся к трудностям отслеживания изменений в законодательных актах (41 % в мире и 32 % РФ), обеспечению содействия уже действующему законодательству (37 % в мире и 40 % РФ), а также подготовленности к соблюдению законодательства (34 % в мире и 24 % РФ). В соответствии с этим для определения электронного документооборота и включения его в единую цифровую среду доверия недостаточно, важно обеспечить юридическую значимость подобных документов, которая выступает как комплексная задача, проходящая все этапы жизненного цикла документа, закрепленного в электронном виде и обеспечивающая ЭДО всеми важными характеристиками (ГОСТ – Р 7.0.8 – 2013 «Свойство документа выступать в качестве подтверждения деловой деятельности либо событий личного характера») [3]. Для обеспечения юридической значимости электронных документов электронную подпись. ЭП связана как с автором, так и самим документом с помощью криптографических методов, и не может быть подделана с помощью обычного копирования, что повышает уровень доверия к электронным документам.

Нормативная база регулирования электронного документооборота с использованием электронной подписи основывается на таких законодательных актах, как: Федеральный закон РФ от 06.04.2011 № 63 «Об электронной подписи» [4]; Федеральный закон РФ от 27.07.2006 № 149 «Об информации, информационных технологиях и защите информации» [5]; Федеральный закон РФ от 27.07.2010 № 210 «Об организации предоставления государственных и муниципальных услуг» [6].

В соответствии с ч. 4 ст. 5 Федерального закона РФ от 06.04.2011 № 63 «Об электронной подписи» существует усиленная квалифицированная электронная подпись, которая обладает такими признаками защищенности данных, как ключ проверки и средства электронной подписи, которые подтверждены. Юридическая значимость электронных документов появляется с использованием усиленной квалифицированной электронной подписи.

Согласно ч. 2 ст. 434 Гражданского кодекса РФ, электронный документ является одной из разновидностей письменной формы документа, но при этом он не обладает большой степенью доверия в отличие от бумажного носителя, уровень безопасности которого выработался за многие годы за счет внедрения государством различных инфраструктур, норм и правил, обеспечивающих хранение бумажных документов, оформление и передачу. Но при этом темпы повышения доверия к электронным носителям ежегодно растут, как, например, изменение в законодательстве о государственных закупках, вступившее в силу с 2019 г., по поводу предоставления закупок в электронной форме с ис-

пользованием в этой сфере Единой информационной системы. То есть, для проведения сделки не нужно требовать от участников закупки бумажных документов при проведении закупки в электронной форме [7].

Одной из нерешенных проблем в сфере повышения доверия к цифровому документообороту является отсутствие законодательного обеспечения долгосрочного хранения документов в электронной форме, создание его копии, а также сохранение его подлинности на долгий срок, поэтому необходимо создать такую нормативную базу и наладить сохранение электронного документа со всеми его ключевыми характеристиками благодаря надежным решениям экспертов в технической сфере.

Создание единого пространства доверия области коммуникационных технологий должны предусматривать виртуальные контакты и сервисы, которые будут надежными, безопасными и удобными. Выполнение этой задачи касается каждого отдельного предприятия и всего государства в целом, так как на сегодняшний день нет сформированного пространства доверия, существует лишь отдельный набор доверительных доменов, что приводит к торможению развития цифровой экономики на территории страны. В связи с этим требуется глобальная реформа по повышению безопасности в области цифровизации, которая неразрывно связана с доверием населения. Одними из направлений реформы можно считать следующее: описание принципов, обеспечивающих сохранение электронного документа на долгосрочный период без потери его юридической силы; предоставление возможности хранения и создания копий электронных документов; нормативное обоснование на создание юридически значимых копий в электронном виде и их архивную конверсию; создание единой открытой библиотеки для использования её органами государственной власти.

Вышеуказанные проблемы по формированию единой среды доверия необходимо решать посредством эффективного вмешательства государства, населения и бизнеса. В этом случае должны быть задействованы все отрасли экономики, новые технологии, нормативное регулирование, кадры и информационная безопасность.

В результате исследования было выявлено, что для повышения безопасности в информационной среде и повышения уровня доверия граждан к цифровизации необходимо внедрять новые инструментари и опции для решения поставленных задач. Рост надежности информационных система возможен только при постоянно обновляющемся наборе функций и методов, использующихся при создании единой цифровой среды доверия. Чтобы вышеуказанные механизмы могли эффективно осу-

ществляться, необходимы высококвалифицированные работники и грамотное руководство. Любая организация, которая будет считать своих сотрудников интеллектуальным капиталом и использовать их знания как преимущества, будет повышать понимание ценности доверия к своей деятельности.

**Список литературы**

1. Указ Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в РФ 2017 – 2030».
2. ЭОС: [Электронный ресурс]. – Режим доступа: <https://www.eos.ru/>, свободный.
3. ГОСТ – Р 7.0.8 – 2013 «Свойство документа выступать в качестве подтверждения деловой деятельности либо событий личного характера».
4. Федеральный закон РФ от 06.04.2011 № 63 «Об электронной подписи».
5. Федеральный закон РФ от 27.07.2006 № 149 «Об информации, информационных технологиях и защите информации».
6. Федеральный закон РФ от 27.07.2010 № 210 «Об организации предоставления государственных и муниципальных услуг».
7. Гражданский кодекс Российской Федерации (ГК РФ).

**ТЕНДЕНЦИИ РАЗВИТИЯ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА**

Белоконева Е.А., Кодинцева В.И.

*Южно-Российский институт управления филиал Российской академии народного хозяйства и государственной службы при Президенте РФ, e-mail: ekaterina.beloneva@yandex.ru*

В данной статье рассмотрены основные направления развития систем электронного документооборота. Приведены и проанализированы данные по применению населением механизмов электронного доступа к услугам. Также в процессе исследования были выявлены перспективные направления развития систем электронного документооборота в государственных органах.

В современном мире практически невозможно представить жизнь человека без использования информационных технологий. По

этой причине, научные исследования связанные с тематикой «цифровизации» имеют большую актуальность. Помимо этого, важным вопросом является развитие концепции электронного правительства Российской Федерации, а также совершенствование проекта «Цифровое правительство», в рамках которого формируется система электронного документооборота между государственными, бюджетными и муниципальными учреждениями.

Концепция «Электронного правительства» предполагает новую форму организации деятельности органов государственной власти, которая обеспечивает за счет применения информационно – коммуникационных технологий новый уровень удобства получения государственных услуг, как организациям, так и гражданами и оперативность получения данных услуг, а также информацию о результатах деятельности государственных органов. По показателю конкурентоспособности в сфере электронного правительства Россия занимает 35-е место в мировом рейтинге, по показателю Цифровой конкурентоспособности – 42-е место [1].

Анализируя данные, полученные Росстатом в отношении людей, перешедших на электронную платформу государственных услуг, можно наблюдать положительную тенденцию числа граждан, которые используют механизм получения государственных и муниципальных услуг путем электронной формы (Рис. 1).

Тем не менее, общие ожидания граждан и бизнеса формируются на основе опыта широкого применения современных технологий. Необходимо довести до конца все реализуемые мероприятия и наметить переход к разработке и реализации стратегий следующего этапа, то есть стратегии перехода к цифровому правительству. В рамках национального проекта «Цифровая экономика» к сроку ее реализации планируется достичь показателей, приведенных в таблице.

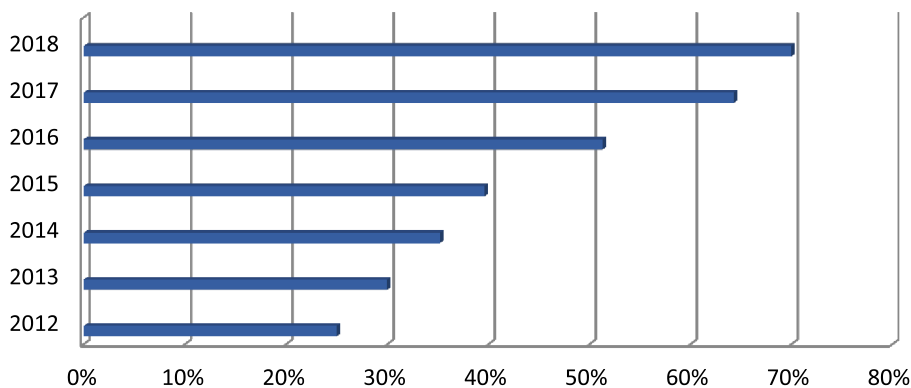


Рис. 1. Доля граждан России, использующих механизм электронного доступа к государственным и муниципальным услугам, % в 2012–2018 гг. [2]