Критерии оценки рисков развития компаний в условиях внедрения финансовых технологий

Е.А. Демьянова,
Финансовый университет,
Москва, Россия
http://orcid.org/0000–0003–4877–8041

Аннотация. Внедрение финансовых технологий в современных условиях оказывает существенное влияние на развитие компаний во всех отраслях экономики. Признанные финансовые авторитеты Российской Федерации и мировые эксперты сходятся во мнении, что финансовые институты всех стран в ближайшие годы кардинально изменятся. Компании, независимо от их размера, формы собственности и сферы деятельности вовлекаются в орбиту новых финансовых технологий, изменяется порядок ведения бизнеса. Правительственная программа 2017–2025 гг. «Цифровая экономика» становится новой точкой отсчета и своеобразным компасом в мире денежного обращения. В связи с внедрением финансовых технологий появляются новые, ранее не рассматриваемые риски, в дополнение к традиционным известным рискам. В статье приводятся примеры принципиально новых подходов к оценке рисков, подчеркивается усиление роли использования объемных массивов данных. Автор рассматривает область новых неохваченных рисков развития компаний, определяет понятия и систематизирует такие риски на макро- и микроуровнях, проводит их сравнительный анализ. В исследовании сравниваются подходы к оценке рисков авторитетных международных экспертных организаций, таких как Всемирный экономический форум, Комитет по организации Комиссии Тредвея (COSO ERM), ведущие международные консалтинговые компании, Банк России. В ранее опубликованных работах другие авторы ограничивались только перечнем новых рисков без разработки конкретных критериев их оценки, подчеркивая в то же время огромный практический потенциал использования таких конкретных критериев оценки. В статье на основании анализа признаков неохваченных рисков развития компаний в условиях внедрения финансовых технологий автор предлагает свое видение признаков классификации критериев оценки и вариант рабочей классификации критериев оценки двух из важнейших неохваченных рисков развития компаний: риска кибербезопасности и риска от использования технологии IoT (Интернет вещей). Под критериями оценки понимается вербальное описание их последствий и «качественное» оценивание вероятностей без перевода в количественные показатели. Эксперты на практике могут использовать данную классификацию с дальнейшим присвоением удельных весов на основании экспертной оценки рисков.

Ключевые слова: неохваченные риски; классификация критериев оценки рисков развития компаний; финансовые технологии; риск кибербезопасности; риск использования технологии IoT (Интернет вещей)

Для цитирования: Демьянова Е.А. Критерии оценки рисков развития компаний в условиях внедрения финансовых технологий // Финансы: теория и практика. 2017. Т. 21. Вып. 4. С. 182–190.
УДК 336
JEL B49; C13
DOI 10.26794/2587-5671-2017-21-4-182-190

Criteria for Assessing Corporate Development Risks Arising with Introduction of Financial Technologies

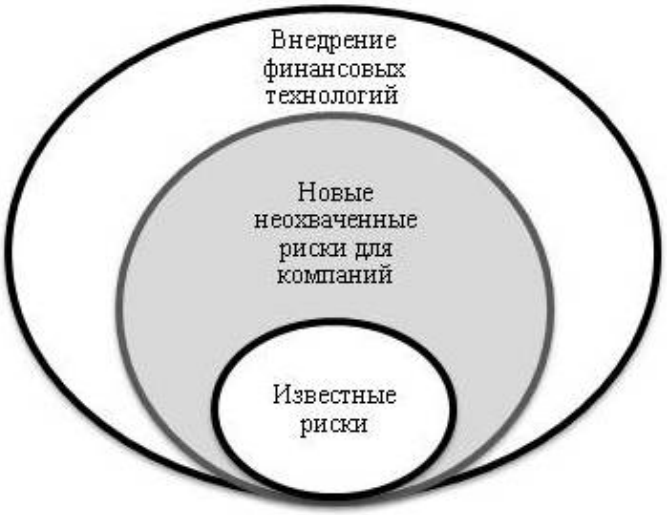
E.A. Demyanova,
Financial University,
Moscow, Russia
http://orcid.org/0000–0003–4877–8041

Abstract. The introduction of financial technologies has a significant impact on the development of companies in all sectors of the economy. The financial gurus of the Russian Federation and world experts agree that the financial institutions of all countries will undergo radical changes in the coming years. Companies, regardless of their size, form of ownership and type of business, are being brought into the orbit of new financial technologies; the ways of doing business are also changing. The government program of 2017–2025 "The Digital Economy" is becoming a new benchmark and a kind of compass in the world of money circulation. The introduction of financial technologies gives rise to new risks not previously considered. The paper provides examples of principally new approaches to risk assessment and emphasizes the increasing importance of using large amounts of data. The author examines the scope of new uncovered risks of corporate development, defines concepts and systematizes such risks at macro and micro levels along with their comparison. The study compares risk assessment approaches of reputed international expert organizations, such as the World Economic Forum, COSO ERM, leading international consulting companies and the Bank of Russia. Authors of previously published works only listed new risks without developing particular criteria for their assessment, though emphasizing the big practical potential of the latter. Based on the analysis of characteristics of non-covered corporate development risks arising with introduction of financial technologies, the author offers her own approach to classification of assessment criteria and a version of the working classification of criteria for assessing two of the most important non-covered corporate development risks: the cyber-crime security risk and the IoT risk. The assessment criteria are understood as a verbal description of risk consequences and a "qualitative" assessment of probabilities without conversion to quantitative indicators. Experts can use this classification in practice with further risk rating on the basis of expert risk assessment.

Keywords: non-covered risks; classification of criteria for assessing corporate development risks; financial technologies; cyber security risk; IoT risk

For citation: Demyanova E.A. Criteria for Assessing Corporate Development Risks Arising with Introduction of Financial Technologies. *Finansy: Teoriya i Praktika = Finance: Theory and Practice*, 2017, vol. 21, issue 4, pp. 182–190.
УДК 336
JEL B49; C13
DOI 10.26794/2587-5671-2017-21-4-182-190

На современном этапе экономического развития на первый план выдвигаются вопросы перехода на новый технологический уровень российской экономики. По поручению Президента Российской Федерации В.В. Путина разрабатывается программа «Цифровая экономика», в рамках которой эксперты планируют создать нормативно-правовое поле, в том числе и для новых финансовых технологий. Финансовые технологии — это цифровые инновационные решения в сфере финансовых услуг, предлагаемые компаниями, использующими новую технологическую платформу, которые конкурируют или сотрудничают с финансовыми институтами. Актуальность новаций подчеркивается в последнее время в научных кругах, так как «изменяется не только сложившийся ландшафт предоставления финансовых услуг» под воздействием новых технологий, но и «отношение к такому понятию, как „деньги"» [1]. В условиях внедрения финансовых технологий вопросы оценки рисков развития компаний приобретают особую актуальность. Традиционный подход к оценке рисков широко используется в оценочной деятельности для оценки стоимости бизнеса, аудиторами, руководством компаний. В нашей стране принято для стоимостной оценки рисков опираться на Федеральный закон от 29.07.1998 № 135-ФЗ «Об оценочной де-



Появление неохваченных рисков развития компаний в условиях внедрения финансовых технологий / New unexplored risks emerge for companies under Fintech implementation

Источник: составлено автором.

Таблица 1/ Table 1

Сравнительный анализ неохваченных рисков макроуровня для компаний / Comparative analysis of non-covered macro-level corporate risks

	Различные риски	Одинаковые риски
ВЭФ	• Риск применения AI (искусственного интеллекта); • риск применения технологии распределенных реестров (блокчейн)	• Киберриск как угроза для стабильности (киберзависимость, атаки); • возможность потери критической информации; • утечка личной/ официальной информации
Банк России	• Угроза финансовой стабильности; • повышение концентрации инновационных игроков, снижение конкурентоспособности существующей бизнес-модели финансовых институтов; • риск дефолта и ликвидности (те же, что и для традиционных кредитных продуктов), однако этот риск в условиях Финтех переносится на конечного клиента; • риск осуществления запрещенных видов деятельности	

Источник: составлено автором.

ятельности в Российской Федерации», нормативные акты Минэкономразвития России, стандарты ГОСТ Р ИСО/МЭК 31010–2011 «Методы оценки риска»; Международный Стандарт ISO 31000:2009.

Комитет спонсорских организаций Комиссии Тредвея выпустил в декабре 2016 г. проект документа «Концептуальные основы внутреннего контроля» для помощи предприятиям и организациям в проведении оценки рисков развития их компаний в новых посткризисных условиях [COSO ERM (2016)], в котором прямо подчеркивается зависимость повышения производительности компаний от качества идентификации и анализа рисков. В этом документе предлагается новый подход к оценке рисков, делается акцент на два дополнительных аспекта риска развития компании: риск того, что стратегия не соответствует заявленной миссии компании и ее ключевым ценностям; а также риск непонимания последствий принятия той или иной стратегии в деталях.

Ведущие консалтинговые компании принимают активное участие в формировании новых подходов к оценке рисков. Так, PwC в обзоре «Всемирный обзор сегмента FinTech» заявляет о формировании

Таблица 2/ Table 2

Сравнительный анализ неохваченных рисков макро- и микроуровней для компаний / Comparative analysis of non-covered macro- and micro-level corporate risks

	Различные риски	Одинаковые риски
Макро (с учетом *табл. 1*)	• Угроза финансовой стабильности; повышение концентрации инновационных игроков, снижение конкурентоспособности существующей бизнес-модели финансовых институтов; • риск дефолта и ликвидности (те же, что и для традиционных кредитных продуктов), однако этот риск в условиях Финтех переносится на конечного клиента; • риск осуществления запрещенных видов деятельности	• Киберриск как угроза для стабильности (киберзависимость, атаки); • возможность потери критической информации; • утечка личной/официальной информации; • риск применения AI (искусственного интеллекта); • риск применения технологии распределенных реестров (блокчейн)
Микро	• Риск применения технологии IoT (Интернет вещей); • риск нехватки специалистов с нужными компетенциями; • несовершенная регуляторная среда	

Источник: составлено автором.

принципиально нового подхода в сегментах страхования, управления активами и частным капиталом, а также революционных изменениях в сфере потребительского и коммерческого кредитования, к которым можно отнести следующее [Электронный ресурс: PwC "Fintech global report", March 2016. URL: http://www.pwc.ru/ru/banking/publications/fintech-global-report-rus.pdf (accessed: 07.05.2017) (In Russ.)]:

1) переход от вероятностной к детерминистской модели оценки рисков (использование нетрадиционных решений сбора данных, включая удаленные устройства, для повышения точности оценки рисков);

2) детализированная количественная оценка рисков (передовые достижения в сфере технологий, направленные на обеспечение возможности количественной оценки рисков с высокой степенью детализации);

3) повышение эффективности выявления и количественной оценки рисков [использование новых моделей и более объемных массивов данных (Big Data) для повышения точности анализа рисков].

Одним из передовых примеров применения нового подхода оценки рисков на практике может служить перевод китайской фирмой CredEx Fintech в марте 2017 г. системы оценки рисков в виртуальное пространство Интернет. Через мобильное приложение за 3 минуты был одобрен и выдан кредит свыше 40 тыс. долл. США с применением технологии идентификации личности и искусственного интеллекта для оценки финансовых и нефинансовых транзакций заемщика. Мировыми учеными ставится вопрос о новой философии оценки рисков финансовых услуг в виртуальном пространстве.

С внедрением финансовых технологий появляются новые, ранее не рассматриваемые риски, в дополнение к традиционным известным рискам. В данном исследовании мы рассматриваем именно эту область новых неохваченных рисков развития компаний, схематично представленную на *рисунке*.

Всемирный экономический форум (ВЭФ) в отчете «Глобальные риски 2017» декларирует начало Четвертой индустриальной революции на пересечении цифровых, биологических и физических технологий, что порождает макориски для бизнеса. С учетом данных материалов и отчета Банка России автором был проведен сравнительный анализ неохваченных рисков для компаний в условиях изменения макросреды под влиянием развития финансовых технологий (*табл. 1*).

Таким образом, можно сделать вывод о том, что в современных экономических условиях на деятельность компаний влияют новые макориски, связанные с развитием новых финансовых технологий. Несмотря на схожесть ряда рисков, часть из них различна в силу неодинаковой степени вовлеченности в процесс развития Финтех.

На микроуровне с точки зрения операционной деятельности компании можно выделить несколько иные риски развития компаний различных секторов экономики. На основании материалов отчета ВЭФ «Будущее Финтеха» и Deloitte&Touche «Глобальное управление рисками» 2017 автором был проведен сравнительный анализ неохваченных рисков макро-

и микроуровней для компаний в условиях развития финансовых технологий (*табл. 2*).

В большинстве исследований в настоящее время приводятся разрозненные примеры рисков на макро- и микроуровнях, возникших в новых экономических условиях внедрения финансовых технологий. Например, М. Свон, исследуя отдельно взятую проблему технологии блокчейна [2], пишет о преимуществах ее применения и возникающих возможностях на уровне государств. О.И. Лаврушин также анализирует новые явления в банковском секторе российской экономики [3], делая акцент на развитии «современных технологий, которые эффективно управляют денежным оборотом на макро- и микроуровне экономических отношений». Ему созвучны работы целой группы финансовых экспертов [4], подчеркивающих, в том числе, и «негативные явления и тенденции» на российском финансовом рынке, который «характеризуется слабым диверсифицированным набором инструментов, неравномерным развитием различных сегментов, ограниченным перечнем участников». Все это указывает на наличие серьезных рисков на макроуровне. В развитие данной тематики присутствия ряда рисков на отечественном рынке, другая группа ученых представила глубокий анализ текущего состояния и перспектив развития финансовой системы России [5]. В статье вскрываются, в том числе, и ее «основные проблемные зоны», подчеркивается необходимость «применения механизмов электронного взаимодействия на финансовом рынке».

Однако нельзя забывать, что для каждой конкретной компании набор рисков будет своим. Анализ показал, что подходы к оценке рисков изменяются и начинают охватывать нефинансовые критерии, словесную информацию из социальных сетей и публикаций в сети Интернет. Поэтому представляется необходимым, по мнению автора, дополнить список типовых рисков, которые учитываются в стоимостной оценке при оценочной деятельности, следующими ранее неохваченными рискам развития компаний в условиях внедрения финансовых технологий (без ранжирования по степени важности): риск кибербезопасности; риск регуляторной среды; риск утечки информации; риск от использования технологий AI (искусственного интеллекта); риск от использования технологий IoT (Интернет вещей); риск от использования технологий DLT (технология распределенного реестра); риск нехватки специалистов с нужными компетенциями; риск поддержания имиджа компании в сети Интернет для потенциального использования в кредитных рейтингах.

Важно отметить, что в ранее опубликованных работах авторы ограничиваются в лучшем случае лишь несистематическим перечнем самих новых рисков, ошибочно игнорируют необходимость разработки конкретных критериев оценки неохваченных рисков. Например, в научном труде А. Шапкина [6] описываются «факторы, влияющие на выбор эффективных решений в условиях риска и неопределенности», приводятся различные методы оценки рисков. Однако конкретные критерии рисков, влияющих на развитие компаний в современных условиях внедрения финансовых технологий, не приводятся. В классическом труде Р. Брейли и С. Майерса [7] хорошо отражено понятие риска, его связь с доходностью, приведены приемы управления риском. Но и в этом фундаментальном труде не уделено достаточного внимания критериям и классификации рисков.

В то же время во многих исследованиях подчеркивается огромный практический потенциал использования конкретных критериев оценки рисков, но сами критерии в научных работах пока нигде не приводятся. Так, в трудах зарубежных авторов, например П. Маршавиласа, Д. Коулоуриотиса, В. Джемини [8], приводится подробный обзор и анализ современных методов оценки рисков как в качественном, так и в количественном выражении, а также делается ценный вывод о превалировании количественных методов анализа риска над прочими. В работе А. Рота [9] предложен общий подход к анализу рисков в информационных технологиях. Однако и в этих работах отсутствуют сами критерии оценки инновационных рисков вообще и в финансовом секторе в частности. Стоит отметить, что Банком России ведется целенаправленная работа по анализу рассматриваемых рисков. Так, особенно отмечается киберриск и связанные с ним угрозы*.

Таким образом, представляется необходимым восполнить данный пробел. Ниже представлена составленная автором классификация критериев оценки двух важнейших неохваченных рисков развития компаний в условиях внедрения финансовых технологий по предложенным автором признакам классификации неохваченных рисков.

РИСК КИБЕРБЕЗОПАСНОСТИ

Авторская классификация критериев оценки риска кибербезопасности приведена в *табл. 3*.

* Центральный Банк Российской Федерации. Обзор финансовой стабильности. № 2, II–III кварталы 2016. с. 37–40 / Central Bank of the Russian Federation. Financial stability review., no. 2, II–III quarters 2016, pp. 37–40. (In Russ.).

Таблица 3/ Table 3

Классификация критериев оценки риска кибер-безопасности / Classification of criteria for cyber security risk assessment

Признак классификации	Критерий оценки риска
Источник воздействия	Внешние целенаправленные хакерские атаки, мошеннические схемы
	Внутренние сотрудники компании намеренно вносят изменения в данные
Сфера охвата	Затронуто одно отделение, местная платформа
	Подвергнуты воздействию несколько филиалов компании, провайдер(ы) облачного хранилища данных
	Подвергнуты воздействию все филиалы компании и головной офис, общий провайдер(ы) облачного хранилища данных
Последствия для деятельности компании в целом	Угроза краткосрочной приостановки деятельности компании в целом или нескольких отделений
	Угроза длительной приостановки деятельности компании в целом или многих отделений
	Угроза полного прекращения деятельности компании
Степень ущерба репутации	Быстро восстанавливаемый со временем — затронуто доверие только одной группы контрагентов; потеря или разглашение части конфиденциальных данных
	Медленно восстанавливаемый — потеря репутации и доверия со стороны нескольких групп клиентов и партнеров; потеря или разглашение значительной доли конфиденциальных данных
	Невосстанавливаемый — полная потеря репутации и доверия со стороны клиентов и партнеров; потеря или разглашение большей доли или утечка всех конфиденциальных данных
Степень материального ущерба	Низкая. Потеря незначительной доли выручки; возмещение незначительных (применительно к данной компании) украденных через кибератаку денежных средств клиенту; возможная повторная покупка незначительных объемов криптовалюты для планируемых операций
	Средняя. Потеря значительной доли выручки; возмещение ощутимых (применительно к данной компании) украденных через кибератаку денежных средств клиенту; возможная повторная покупка ощутимых объемов криптовалюты для планируемых операций
	Высокая. Потеря всей выручки; возмещение существенно значительных (применительно к данной компании) украденных через кибератаку денежных средств клиенту; возможная повторная покупка существенных объемов криптовалюты для планируемых операций
Степень ущерба третьим лицам	Низкая. Кибератака нанесла незначительный вред программному обеспечению, что вызвало сбой в работе станков и оборудования, привело к порче материала и заготовок, нанесло вред окружающей среде, привело к травмам сотрудников, находящихся в зоне сбоя
	Средняя. Кибератака нанесла существенный вред программному обеспечению, что вызвало сбой в работе станков и оборудования, привело к порче материала и заготовок, нанесло вред окружающей среде, привело к травмам сотрудников, находящихся в зоне сбоя
	Высокая. Кибератака нанесла обширный вред программному обеспечению, что вызвало сбой в работе станков и оборудования, привело к порче материала и заготовок, нанесло вред окружающей среде, привело к травмам сотрудников, находящихся в зоне сбоя

Окончание таблицы 3 / End of Table 3

Признак классификации	Критерий оценки риска
Степень вероятности возникновения	Низкая. В компании действует система мер предотвращения и снижения риска, политики исправно выполняются и постоянно обновляются
	Средняя. В компании действует незамкнутая система мер предотвращения и снижения риска, политики не всегда исправно выполняются и редко обновляются
	Высокая. В компании отсутствует система мер предотвращения и снижения риска, политики не выполняются и не обновляются
Прогноз степени снижения последствий возникновения	Высокий. В компании соблюдаются все политики безопасности, проводится мониторинг исполнителей; применяются усиленные криптографические методы и защищенные протоколы; проводится постоянная проверка партнеров, предоставляющих виртуальные услуги; введено усиление мер по идентификации клиентов; происходит регулярное резервное копирование; киберриск застрахован
	Средний. В компании частично соблюдаются политики безопасности, проводится мониторинг исполнителей выборочно; частично применяются усиленные криптографические методы и защищенные протоколы; проводится выборочная проверка партнеров, предоставляющих виртуальные услуги; введено усиление мер по идентификации клиентов; происходит спорадическое резервное копирование; киберриск не застрахован
	Низкий. В компании не соблюдаются политики безопасности, не проводится мониторинг исполнителей; не применяются усиленные криптографические методы и защищенные протоколы; не проводится проверка партнеров, предоставляющих виртуальные услуги; не введено усиление мер по идентификации клиентов; не происходит резервное копирование; киберриск не застрахован
Влияние на бухгалтерский баланс компании	Активы. Влияние на дебиторскую задолженность через финансовые технологии, факторинг дебиторской задолженности
	Пассивы. Влияние на краткосрочную кредиторскую задолженность через финансовые технологии P2P (равный-равному) финансирование
	Раздел «Капитал» через финансовые технологии краудфандинг

Источник: составлено автором.

РИСК ОТ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ IOT (ИНТЕРНЕТ ВЕЩЕЙ)

Прежде, чем привести классификацию критериев оценки данного риска, представляется необходимым подчеркнуть его глубину и актуальность, пояснить выбор именно этого риска для оценки развития компаний в современных условиях. Технология IoT включает сенсорные устройства (промышленные роботы, телематика, нательные электронные устройства, самоуправляемые автомобили, грузовые дроны) и применяется банками, страховыми компаниями, промышленными и сельскохозяйственными предприятиями, торговыми компаниями. Например, для мониторинга предметов залога, складских запасов или скота; для проведения оценки ущерба путем аэрофотосъемки; в автостраховании на основании пробега и по факту частоты использования; при использовании сенсорных устройств для платежей через подключенные мобильные приложения пользователей; для доставки наличных денег банками. Оказалось, что 70–76% общеупотребимых устройств IoT уязвимы, что говорит о значимости проблемы (*табл. 4*).

ВЫВОДЫ

Оценочная деятельность в условиях развития финансовых технологий приобретает новые черты. В частности, появляются ранее не принимаемые во внимание риски деятельности компаний. Такие неохваченные риски требуют оценки, выявления степени их влияния на величину стоимости бизнеса. Требуется дальнейшая классификация критериев оценки рисков, а также совершенствование методов оценки рисков в условиях внедрения финансовых технологий.

В рамках настоящего исследования автором определены понятия неохваченных рисков развития компаний в условиях внедрения финансовых технологий и признаки классификации, приведена авторская классификация критериев оценки двух

Таблица 4 / Table 4

Классификация критериев оценки риска от использования технологии IoT (Интернет вещей) / Classification of criteria for IoT risk assessment

Признак классификации	Критерий оценки риска
Степень уязвимости устройств IoT из-за подключения к глобальной сети	Низкая. Обеспечена полная степень шифрования сообщений во время работы устройства и «в покое» с использованием новейших достижений
	Средняя. Обеспечена выборочная степень шифрования сообщений во время работы устройства и «в покое»
	Высокая. Не обеспечена степень шифрования сообщений во время работы устройства и «в покое» вовсе либо обеспечена устаревшими протоколами
Вероятность утечки личной/официальной информации	Низкая. Соблюдение всех протоколов безопасности для повышения уровня защиты устройств Io T. Потеря или разглашение конфиденциальных данных одной группы контрагентов
	Средняя. Неполное соблюдение протоколов безопасности для повышения уровня защиты устройств Io T. Потеря или разглашение конфиденциальных данных нескольких групп контрагентов
	Высокая. Несоблюдение протоколов безопасности для повышения уровня защиты устройств Io T. Потеря или разглашение всех конфиденциальных данных
Последствия для деятельности компании в целом	Угроза краткосрочной приостановки деятельности компании в целом или нескольких отделений. Приняты все меры по персональной идентификации пользователей. Данный риск применения IoT застрахован
	Угроза длительной приостановки деятельности компании в целом или многих отделений. Приняты не все меры по персональной идентификации пользователей. Данный риск применения IoT частично застрахован
	Угроза полного прекращения деятельности компании. Меры по персональной идентификации пользователей не приняты. Данный риск применения IoT не застрахован
Вероятность высвобождения сотрудников из-за автоматизации	Низкая. Устройства IoT не применяются
	Средняя. Устройства IoT применяются изредка
	Высокая. Устройства IoT широко применяются компанией
Вероятность нарушения в работе систем IoT из-за их сложности и оказание воздействия на жизнь и здоровье человека	Низкая. Выделены отдельные частотные полосы и платформы для IoT; соблюдаются все правила работы с IoT; каналы связи между «умным» устройством и входом в облачное хранилище защищены; угрозы жизни и здоровью человека не возникает
	Средняя. Выделены отдельные частотные полосы и платформы для IoT; правила работы с IoT нарушаются; каналы связи между «умным» устройством и входом в облачное хранилище ненадежно защищены; возникает угроза причинения ущерба здоровью человека
	Высокая. Отдельные частотные полосы и платформы для IoT не выделены; правила работы с IoT не соблюдаются; каналы связи между «умным» устройством и входом в облачное хранилище не защищены; возникает угроза жизни и здоровью человека

Источник: составлено автором.

наиважнейших неохваченных рисков развития компаний в условиях внедрения финансовых технологий: риска кибербезопасности и риска от использования технологии IoT (Интернет вещей).

СПИСОК ИСТОЧНИКОВ

1. Масленников В., Федотова М., Сорокин А. Новые финансовые технологии меняют наш мир // Вестник Финансового университета. 2017. Т. 21. № 2. С. 6–11.
2. Свон М. Блокчейн. Схема новой экономики. М.: Олимп-бизнес, 2017.
3. Лаврушин О. Новые явления в развитии кредита и институционной структуры банковского сектора // Банковское дело. 2017. № 2. С. 14–19.
4. Абрамова М., Ковалева Н., Лаврушин О., Рубцов Б., Цыганов А. Основные направления развития финансового рынка Российской Федерации в среднесрочной перспективе: мнение экспертов // Экономика. Налоги. Право. 2016. № 4. С. 6–11.
5. Абрамова М., Гончаренко Л., Дубова С., Лаврушин О., Ларионова И., Масленников В., Рубцов Б., Цыганов А. Текущее состояние и перспективы развития финансовой системы России // Экономика. Налоги. Право. 2017. № 2. С. 6–21.
6. Шапкин А., Шапкин В. Экономические и финансовые риски. М.: Дашков и Ко., 2016. 543 с.
7. Брейли Р., Майерс С. Принципы корпоративных финансов. М.: Олимп-бизнес, 2004. 977 с.
8. Marhavilas P.K., Koulouriotis D., Gemeni V. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009. Journal of Loss Prevention in the Process Industies, 2011, no. 24, pp. 477–523. Doi: 10.1016/j.jlp.2011.03.004
9. Rot A., IT Risk Assessment: Quantitative and Qualitative Approach. Proc. of the World Congress on Engineering and Computer Science 2008 WCECS2008, October 22–24, 2008. San Francisco, USA.

REFERENCES

1. Maslennikov V., Fedotova M., Sorokin A., New financial technologies change our world. *Vestnik Finansovogo universiteta = Bulletin of Financial University*, vol. 21, no. 2, 2017, pp. 6–11. (In Russ.).
2. Svon M. Blockchain. Blueprint for a New Economy. Moscow: Olymp-Business Publ., 2017.
3. Lavrushin O. New substancies in loans development and institutional structure of the banking sector. *Bankovskoe delo = Banking*, 2017, no. 2, pp. 14–19. (In Russ.).
4. Abramova M., Kovaleva N., Lavrushin O., Rubtsov B., Tsyganov A. The Mid-Term Trends in the Russian Financial Market Development: Expert Opinion. *Ekonomika. Nalogi. Pravo = Economy. Taxes. Law,* 2016, no. 4, pp. 6–11. (In Russ.).
5. Abramova M., Goncharenko L., Dubova S., Lavrushin O., Larionova I., Maslennikov V., Rubtsov B., Tsyganov A. The financial system of Russia: current state and development prospects. *Ekonomika. Nalogi. Pravo = Economy. Taxes. Law,* 2017, no. 2, pp. 6–21. (In Russ.).
6. Shapkin A., Shapkin V. Economic and financial risks. Moscow: Dashkov and Ko. Publ., 2016, 543 p. (In Russ.).
7. Brealey R., Myers S. [Principles of Corporate Finance. 7th ed. International Edition, McGraw-Hill, Inc., 2003]. Russian Ed.: *Principles of Corporate Finance*. Moscow: Olymp-Business Publ., 2004, 977 p.
8. Marhavilas P.K., Koulouriotis D., Gemeni V. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009. *Journal of Loss Prevention in the Process Industies*, 2011, no. 24, pp. 477–523. Doi: 10.1016/j.jlp.2011.03.004.
9. Rot A., IT Risk Assessment: Quantitative and Qualitative Approach. Proc. of the World Congress on Engineering and Computer Science 2008 WCECS2008, October 22–24, 2008. San Francisco, USA.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Екатерина Александровна Демьянова — соискатель Департамента корпоративных финансов и корпоративного управления, Финансовый университет при Правительстве Российской Федерации, Москва, Россия
EADemyanova@ya.ru

ABOUT THE AUTHOR

Ekaterina Aleksandrovna Demyanova — is external PhD student at the Corporate Finance and Corporate Management Department, Financial University under the Government of the Russian Federation, Moscow, Russia
EADemyanova@ya.ru