УДК 004.056 DOI: 10.26102/2310-6018/2020.31.4.038

Управление рисками информационной безопасности цифровых продуктов финансовой экосистемы организации

А.В. Царегородцев, С.В. Романовский, С.Д. Волков, В.Е. Самойлов
Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный лингвистический университет»
Москва, Российская Федерация

Резюме: В условиях цифровых и технологических вызовов, изменений отношения между участниками рынка возникают модифицированные виды угроз информационной безопасности, источниками которых являются инновационные финансовые сервисы и их комбинации. Это связано с новейшей тенденцией трансформации традиционных сервисных моделей в финансовые экосистемы, которые являются важной частью эволюции финансового сектора. В контексте риска информационной/кибербезопасности, продукт финансовой экосистемы следует определять как архитектурно завершённую информационно-коммуникационную технологию, обеспечивающую потребность клиента организации наличием предопределённых и реализуемых полезных свойств. Трансформация факторов риска информационной/кибербезопасности неизбежно влияет на необходимость пересмотра подходов к оценке рисков, концентрируя внимание специалистов по информационной безопасности на цифровых финансовых сервисах – продуктах финансовых экосистем. Задачей оценки риска информационной/кибербезопасности продукта финансовой экосистемы является не столько предсказание будущего состояния самого продукта или финансовой экосистемы, сколько осознанное управление в рамках реализации конкретных сценариев. Тема исследования посвящена описанию отдельных аспектов новой модели управления рисками информационной безопасности в условиях развития финансовых экосистем. Рассмотрены проблемы использования классической модели анализа рисков информационной/кибербезопасности. Предложен метод оценки риска, учитывающий особенности гетерогенной среды финансовых экосистем и динамики факторов риска.

Ключевые слова: экосистема, трансформация, информационная безопасность, кибербезопасность, риски информационной безопасности, ключевые индикаторы риска, цифровой профиль, финансовая экосистема, цифровые технологии.

Для цитирования: Царегородцев А.В., Романовский С.В., Волков С.Д., Самойлов В.Е. Управление рисками информационной безопасности цифровых продуктов финансовой экосистемы организации. *Моделирование, оптимизация и информационные технологии.* 2020;8(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=888 DOI:10.26102/2310-6018/2020.31.4.038

Digital products' information security risk management in the organization financial ecosystem

A.V. Tsaregorodtsev, S.V. Romanovskiy, S.D. Volkov, V.E. Samoylov
Moscow State Linguistic University,
Moscow, Russian Federation

Abstract: In the context of digital and technological challenges, changes in relations between market participants, modified types of information security threats arise, the sources of which are innovative financial services and their combinations. Such types appear due to the recent trend of transforming traditional service models into financial ecosystems, essential in the financial sector's evolution. In the context of information / cyber security risk, the product of the financial ecosystem should be defined as an architecturally complete information and communication technology that meets the needs of the

organization's client with the presence of predefined and implemented useful properties. The transformation of information security risk factors inevitably affects the need to revise approaches to risk assessment, focusing on information security specialists on digital financial services - products of financial ecosystems. The task of assessing the information / cybersecurity risk of a product of a financial ecosystem is not so much predicting the future state of the product itself or the financial ecosystem, but deliberate management within the framework of the implementation of specific scenarios. The research topic is devoted to describing certain aspects of the new model of information security risk management in the development of financial ecosystems. The problems of using the classical model of information / cyber security risk analysis are considered. A risk assessment method is proposed that takes into account the peculiarities of the heterogeneous environment of financial ecosystems and the dynamics of risk factors.

Keywords: ecosystem, transformation, information security, cybersecurity, information security risks, key risk indicators, digital profile, financial ecosystem, digital technologies.

For citation: Tsaregorodtsev A.V., Romanovskiy S.V., Volkov S.D., Samoylov V.E. Digital products' information security risk management in the organization financial ecosystem. *Modeling, optimization and information technology*. 2020;8(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=888 DOI:10.26102/2310-6018/2020.31.4.038 (In Russ).

.

Введение (Introduction)

Современная финансовая экосистема представляет собой совокупность цифровых сервисов и услуг из различных областей деятельности человека – «продуктов экосистемы», объединённых в рамках одной организации, чаще всего, вокруг технологической платформы, которая обеспечивает «единую точку входа» для всех услуг и сервисов.

Одними из первых, кто приступил к исследованиям и внедрению моделей финансовых экосистем, стали организации банковской системы, которые в конце XX века, на исходе третьей индустриальной революции, столкнулись с некоторым снижением спроса на классические банковский продукты и сервисы, что сделало необходимым поиск новых моделей построения отношений с клиентами [1]. Переосмысление подходов к взаимодействию с клиентами основано на понимании того, что для развития коммерческих отношений организации банковской системы должны перейти от удовлетворения транзакционных потребностей к удовлетворению нефинансовых, эмоциональных духовных потребностей людей, создавать нестандартные продукты, которые меняют стереотипы классических отношений «банк-клиент».

Развитие сервисных моделей, их преобразование в цифровые продукты дало импульс к их концентрации на цифровых площадках финансовых экосистем. Развитие финансовых экосистем неразрывно связано с развитием информационных технологий и инструментов цифровизации – механизмов преобразования информации в цифровую форму. Среди прочих технических возможностей, которые способна предоставить современная финансовая экосистема своим участникам можно выделить систему идентификации клиентов, быстрый обмен данными, единые программные интерфейсы и сервисы, включая информационную и кибербезопасность, возможность формирования продуктового портфеля для B2B и B2C сегментов финансового рынка [2].

Однако, в условиях цифровизации решения на базе технологических инноваций могут выступить как драйвером, так и генератором новых угроз и рисков системе обеспечения информационной безопасности финансовой организации, в том числе за счёт использования цифровых продуктов финансовых экосистем. Инновационные

технологические решения, которые способствуют модификации институциональных отношений, влияют на политические, информационные, технологические, экономические, рыночные и правовые факторы. В эпоху трансформации приоритетов организаций, связанной с цифровизацией и развитием финансовых экосистем эти факторы, следует рассмотреть с позиции риска, с целью оценить степень влияния результатов трансформационных процессов на внешнюю и внутреннюю информационную среду организаций.

Материалы и методы (Materials and Methods)

Для оценки степени влияния результатов трансформационных процессов на внешнюю и внутреннюю информационную среду организаций использовались: методы логического анализа, сравнительного анализа, классификация, дедукция, методы синтеза.

Для исследования использовались государственные стандарты, отчёты и статистическая информация ЦБ РФ, монографии, научные публикации, результаты международных научно-практических конференций.

Результаты (Results)

Систему управления рисками можно охарактеризовать как процесс поиска, идентификации, измерения и принятия мер в отношении конкретных событий риска информационной/кибербезопасности. Задачей оценки риска информационной/кибербезопасности продукта финансовой экосистемы является не столько предсказание будущего состояния самого продукта или финансовой экосистемы, сколько осознанное управление в рамках реализации конкретных сценариев.

Современные сценарии риска чрезвычайно сложны, лица принимающие решения, полагаясь на данные и результаты анализа рисков, могут совершить ошибку, вследствие использования некачественных данных и информации. Данные поступают в больших объемах и высокой скоростью, без их мгновенной предобработки и визуализации полученных результатов обнаружение закономерностей или аномалий в поведении продуктов и финансовых экосистем становится практически невозможным. Вместе с тем, следует отметить, что внедрение статических процессов и процедур оценки, которые предлагают большинство современных методик, основанных, в том числе, на подходах ГОСТ Р ИСО/МЭК 27005-2010, СТО БР ИББС, NIST-RMF, AS/NZS 4360:2004, терпят неудачу именно по причине отсутствие учёта динамической составляющей в оценке риска информационной/кибербезопасности, которая характеризует скорость развития события риска или, иными словами, скорость распространения возможного аномального события в среде финансовой экосистемы.

Традиционный подход к оценке рисков информационной/кибербезопасности основан на двумерном представлении зависимостей воздействия (Impact) и вероятности (Likelihood). Графически, данная модель может быть представлена в виде двумерной «тепловой карты», где на горизонтальной оси откладывают рассчитанное значение величины потерь от реализации события риска, на вертикальной оси откладывают значение вероятности того, что риск материализуется и станет определённым событием (risk event) для организации. В данном случае определяют 16 возможных значений величин риска информационной/кибербезопасности (Рисунок1) для каждой исследуемой области.

Проблема с использованием двумерных моделей заключается в их ограниченности и отсутствии преимуществ, необходимых для надлежащего анализа и визуализации данных с учётом динамики происходящих событий. Статические данные могут вводить в заблуждение лиц, принимающих решение, предоставляя устаревшую информацию.

Добавляя третью переменную - скорость (Velocity), мы вводим новую визуальную фазу с 64 возможными значениями величин риска информационной/кибербезопасности.

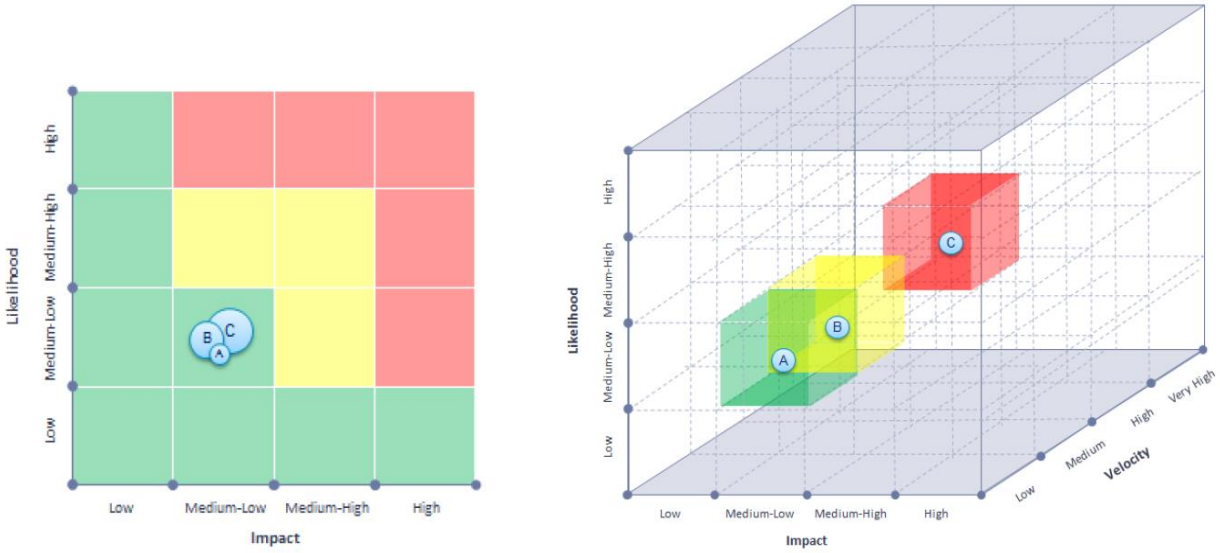

Рисунок 1 – Визуализация результатов оценки риска информационной безопасности - «тепловая карта риска»

Figure 1 – Visualization of information security risk assessment results - "risk heat map"

На оси «Velocity» откладывается время, которое потребуется для того, чтобы событие риска материализовалось («возможное время до наступления события»). Чем выше значение «Velocity», тем меньше времени для реализации корректирующих мер.

Данный показатель способствует дифференциации возможных значений величин риска информационной/кибербезопасности, которые могут иметь одинаковую вероятность (Likelihood) и воздействие (Impact), но различаться по уровням критичности вследствие разной скорости реализации событий (Velocity). Объекты оценки (продукты экосистемы) преобразуются в модели вида трёхмерных кластеров (risk clusters), как показано на Рисунке1. (A,B,C), определённым образом формируя самостоятельные области оценки риска, которые объединены логикой исследуемой финансовой экосистемы.

$$R = L \times I \times V \qquad (1)$$

Где,

R - величина риска информационной/кибербезопасности;
L - вероятность наступления события риска;
I - величина воздействия риска на объект оценки;
V - скорость реализации события риска.

Для расчёта совокупного риска информационной/кибербезопасности финансовой экосистемы (R_u), состоящей из n-кластеров (продуктов финансовой экосистемы), необходимо определить наборы, присущих каждому кластеру (R_k) - частных, внешних (R_{no}) и внутренних (R_{ni}) групп рисков, где R_k=$\{R_{ni}, R_{no}\}$, оценить риски, ранжировать их по уровню критичности, с учётом уровня «Velocity». Поскольку частные показатели могут иметь различную размерность, то совокупный риск целесообразно определять как среднее геометрическое из уровней частных рисков по показателям, формирующий уровень риска в каждом кластере:

$$R_u = \sqrt[i]{\prod_{k=1}^{i} R_k} \qquad (2)$$

Где,

R_u - совокупный уровень риска информационной безопасности финансовой экосистемы;

R_k - частный показатель риска информационной безопасности кластера (продукта экосистемы);

i - количество частных показателей риска информационной безопасности кластера (продукта экосистемы).

Независимо от того, проводится ли оценка риска количественно или качественно, возможность оценки скорости риска дает более полное и глубокое представление о потенциальной угрозе. Данный метод оценки определённым образом меняет подход к формированию системы управления рисками ИБ – стратегиями, планами реагирования, эскалациями, позволяя более полно и точно определить природу риска, а также расставить приоритеты в отношении распределения ресурсов на снижение рисков.

Обсуждение (Discussion)

Риск информационной/кибербезопасности продуктов финансовой экосистемы рассматривается как компонента структуры операционного риска финансовой организации (Рисунок 2), управляется в рамках интегрированной системы управления рисками, совместно с другими видами риска организации. Требования информационной/кибербезопасности формируют базовый уровень для оценки риска на этапах жизненного цикла продукта финансовой экосистемы, что должно быть отражено в соответствующем профиле риска информационной/кибербезопасности, наряду с контекстом организации и описанием самого продукта финансовой экосистемы. Система управления рисками информационной/кибербезопасности формулируется в контексте стратегических инициатив обеспечения информационной/кибербезопасности и операционной устойчивости организации.

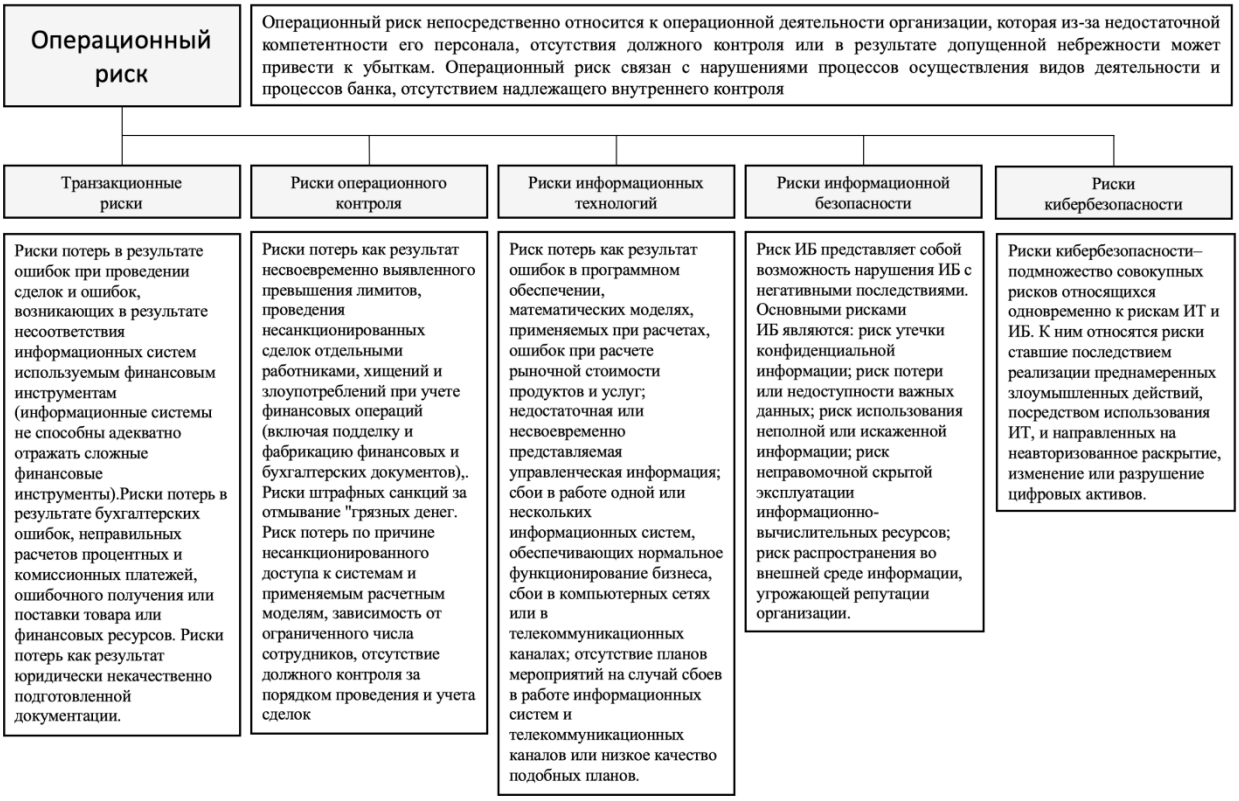

Рисунок 2 – Риск информационной безопасности в структуре управления операционным риском финансовой организации

Figure 2 – Information security risk in the operational risk management structure of a financial organization

Контекст обеспечения информационной/кибербезопасности продукта финансовой экосистемы, наряду с процессом управления операционными рисками, включает точки зрения и ожидания заинтересованных сторон, в отношении уровня зрелости обеспечения информационной/кибербезопасности, категории технологических рисков, рисков третьих сторон, киберустойчивость, а также категории и уровни критичности активов, связанный с ними возможный ущерб [3]. Процесс управления рисками информационной/кибербезопасности должен включать в себя условия нормального режима работы продукта финансовой экосистемы и условия работы в режиме непредвиденной или чрезвычайной ситуации, учитывать влияние рисков информационной/кибербезопасности на возможные потери, связанные с невозможностью использования всех преимуществ продукта финансовой экосистемы.

Угрозы информационной/кибербезопасности определяются относительно тех событий, которые могут отрицательным образом влиять на достижение целей продукта финансовой экосистемы. Выявление рисков информационной/кибербезопасности основывается на дифференцированных результатах исследования свойств продукта финансовой экосистемы. Результаты исследований используются для идентификации угроз информационной/кибербезопасности как продукта, так и финансовой экосистемы в целом.

Вероятность возникновения и последствия каждого идентифицированного риска информационной/кибербезопасности оцениваются с использованием имеющихся данных об угрозах и уязвимостях по всему спектру событий и инцидентов, которые связаны с продуктом финансовой экосистемы, и обоснованных предположений в

отношении событий, инцидентов, прогнозов потенциальных угроз и вероятности их реализации. Данные и информация для подготовки прогнозов должны быть достоверны и воспроизводимы.

Управление риском информационной/кибербезопасности продукта финансовой экосистемы следует определять как процесс, состоящий из следующих ключевых компонент: идентификация риска, анализ риска, обработка риска, мониторинг и контроль профиля риска, аудит риска [7]. Процесс управления риском продукта финансовой экосистемы заключается в систематическом анализе операционных процессов организации и результатов обработки событий информационной/кибербезопасности с целью проведения оценки риска, разработки и использования механизмов, направленных на снижение уровня риска на всех стадиях жизненного цикла продукта финансовой экосистемы.

В контексте риска информационной/кибербезопасности, продукт финансовой экосистемы следует определять как архитектурно завершённую информационно-коммуникационную технологию, обеспечивающую потребность клиента организации наличием предопределённых и реализуемых полезных свойств.

Контекст риска информационной/кибербезопасности должен быть сфокусирован на понимании бизнес-логики продукта финансовой экосистемы, при условии взаимодействия с группами риска в рамках системы интегрированного управления рисками финансовой организации, защите активов, защите инфраструктуры, защите персональных данных, обеспечении информационной безопасности программного обеспечения и приложений, обеспечении информационной безопасности автоматизированных систем и автоматизированных рабочих мест пользователей, защите данных, безопасности облачной инфраструктуры, обеспечении информационной безопасности объектов критической информационной инфраструктуры [8].

С целью поддержания риска на приемлемом уровне необходимо разрабатывать профили риска и контрольные среды для мониторинга состояния риска информационной безопасности продуктов финансовой экосистемы.

К ключевым показателям реализации процесса управления риском продукта экосистемы следует отнести:

– наличие определённых требований информационной безопасности и стратегии управления рисками продукта финансовой экосистемы;

– наличие определённого перечня угроз информационной безопасности продукта финансовой экосистемы, способность их выявления и наличие инструментов анализа;

– наличие разработанных стратегий обработки рисков информационной безопасности продукта финансовой экосистемы их применимость и приоритетность использования;

– наличие релевантных методик оценки риска информационной безопасности продукта финансовой экосистемы и результатов их использования в целях мониторинга изменений величины риска и учёта прогресса в обработке рисков;

– наличие процесса регистрации в профиле рисков и обработки событий риска информационной безопасности продукта финансовой экосистемы [9].

Пороговые значения и условия принятия риска информационной/кибербезопасности, определяются для всех классов и типов информационных активов продуктов финансовой экосистемы и соотносятся с контекстом управления рисками [10]. Пороговые значения риска информационной безопасности и его ключевые индикаторы, отражают данные объективного контроля

(метрики) и мнение заинтересованных сторон в терминах нормального осуществления операционной деятельности организации и обеспечение всех её функций.

Профиль риска информационной/кибербезопасности должен содержать данные в отношении риска продукта финансовой экосистемы. Информация, составляющая профиль риска, содержит полную информацию о продукте, перечень угроз и уязвимостей в отношении информационных активов, входящих в состав продукта [11]. Профиль риска носит динамический характер и обновляется в случае любого отклонения от уровня приемлемого риска и фиксирует показатели, влияющие на положительную или отрицательную динамику риска информационной/кибербезопасности продукта. Профиль риска позволяет отслеживать величину риска и волатильность уровня риска по всем параметрам, в том числе, в терминах идентификации, анализа, оценки, обработки и мониторинга в отношении целевого уровня риска.

Целевой уровень риска информационной/кибербезопасности и степень отклонения от целевого уровня риска обеспечивают принятие решений о возможностях использования продукта финансовой экосистемы заинтересованными сторонами на протяжении всего жизненного цикла продукта. Результаты оценки риска, любые отклонения от целевых параметров уровня риска, результаты обратной связи от потребителей продукта должны предоставляться соответствующим заинтересованным сторонам в соответствии с достигнутыми договорённостями (контракты, обязательства, договора и т.п.), в целях обеспечения ведения совместной деятельности. Целевой уровень риска информационной безопасности продукта экосистемы, любые отклонения от целевого уровня риска, волатильность показателей уровня риска, являются основанием для принятия решений о качестве продукта и подтверждения обязательств по отношению к требованиям заинтересованных сторон.

Заключение (Conclusion)

Цифровая трансформация создает многочисленные преимущества для потребителей финансовых услуг, неизбежно увеличивает качество, скорость, доступность взаимодействия потребителей финансовых услуг и финансовых организаций, но вместе с тем создает дополнительные риски. Рост масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, является глобальным трендом, требующим скоординированных усилий регуляторов, правоохранительных органов, организаций кредитно-финансовой сферы и потребителей финансовых услуг. Крупномасштабные кибератаки наносят значительный экономический ущерб, приводят к изменениям в геополитических отношениях и снижению уровня доверия к информационно-телекоммуникационной сети «Интернет». Кибератаки на цифровые финансовые системы способны спровоцировать финансовый кризис. В Отчете Всемирного экономического форума по глобальным рискам 2019 года кибератаки определены как разновидность базового глобального технологического риска. Трансформация системы управления рисками информационной/кибербезопасности продуктов финансовой экосистемы позволит существенно улучшить качество обеспечения информационной безопасности финансовых организаций, выстроить тактику преодоления и снижения рисков информационной/кибербезопасности, способствовать устойчивому развитию финансовых экосистем.

ЛИТЕРАТУРА

1. Васин С.М. Гамидуллаева Л.А. Концептуальные вопросы управления инновационной системой. *Russian Journal of Management*. 2015;3(4):342-351.
2. Гамидуллаева Л.А. Опыт государственной поддержки бизнес-инкубирования за рубежом и возможности его адаптации в России. *Вестник Томского государственного университета*. 2013;369:122-125.
3. Толстых Т.О., Агаева А.М. Экосистемный подход как концепция инновационного развития экономики. *Наука сегодня: вызовы и решения*: материалы Междунар. науч.-практ. конф. (г. Вологда, 29 января 2020 г.). – Вологда: ООО «Маркер», 2020;1:73.
4. Толстых Т.О., Шкарупета Е.В. Влияние человеческого потенциала на формирование цифровой экосистемы в рамках кросс-отраслевой трансформации. *Актуальные проблемы развития хозяйствующих субъектов, территорий и систем регионального и муниципального управления*: материалы XIV Междунар. науч.-практ. конф. 2019;1:210-213.
5. Nolan A., Guellec D. *The digitalisation of science, technology and innovation. An overview of key developments and policies.* OECD, DSTI/STP. 2019;1:14.
6. OECD (2019). University-Industry Collaboration: New Evidence and Policy Options. – Paris : OECD Publishing, 2019.
7. Клейнер Г.Б. Социально-экономические экосистемы в контексте дуального пространственновременного анализа. *Экономика и управление: проблемы и решения*. 2018;5(5):5-13.
8. Technical risk assessment handbook: Version 1.1. *Australian Government: Department of defence. Defence Science and Technology organization*. – Canberra. 2016;1:42.
9. Стандартизация в Российской Федерации. Основные положения: ГОСТ Р 1.0–2012. – Взамен ГОСТ Р 1.0-2004; введ. 01.07.2013.
10. *Менеджмент риска. Термины и определения:* ГОСТ Р 51897–2011/Руководство ИСО 73:2009. – Взамен ГОСТ Р 51897-2002; введ. 01.12.2012.
11. *Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019-2021 годов.* Центральный банк Российской Федерации. Режим доступа: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения: 01.10.2020).

REFERENCES

1. Vasin S.M. Gamidullaeva L.A. Conceptual issues of management of an innovative system . *Russian Journal of Management*. 2015;3(4):342-351.
2. Gamidullaeva L.A. Experience of state support for business incubation abroad and the possibility of its adaptation in Russia . *Bulletin of Tomsk State University*. 2013;369:122-125.
3. Tolstykh T.O., Agaeva A.M. Ecosystem approach as a concept of innovative development of the economy . *Science today: challenges and solutions: materials of Intern. scientific-practical conf.* (Vologda, January 29, 2020). - Vologda: LLC "Marker". 2020;1:73.
4. Tolstykh T.O., Shkarupeta E.V. The impact of human potential on the formation of a digital ecosystem in the framework of cross-industry transformation . *Actual problems of the development of economic entities, territories and systems of regional and municipal management: materials of the XIV Intern. scientific-practical conf.* 2019;1:210-213.
5. Nolan A., Guellec D. The digitalization of science, technology and innovation. *An overview of key developments and policies* . OECD, DSTI / STP.2019;1:14.

6. OECD (2019). University-Industry Collaboration: New Evidence and Policy Options. - Paris: OECD Publishing, 2019.
7. Kleiner G.B. Socio-economic ecosystems in the context of dual spatial-temporal analysis . *Economics and Management: Problems and Solutions.* 2018;5(5):5-13.
8. Technical risk assessment handbook: Version 1.1 . Australian Government: Department of defense. *Defense Science and Technology organization.* - Canberra. 2016;1:42.
9. Standardization in the Russian Federation. Basic provisions: GOST R 1.0–2012. - Instead of GOST R 1.0-2004; entered 01.07.2013.
10. *Risk management. Terms and definitions:* GOST R 51897–2011/ ISO Guide 73: 2009. - Instead of GOST R 51897-2002; entered 01.12.2012.
11. *The main directions of development of information security in the credit and financial sector for the period 2019-2021*. Central Bank of the Russian Federation. Access mode: https://cbr.ru/Content/Document/File/83253/onrib_2021. (date of access: 01.10.2020).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Царегородцев Анатолий Валерьевич, доктор технических наук, профессор, проректор по развитию и информатизации, ФГБОУ ВО МГЛУ, Москва, Российская Федерация,
e-mail: avtsaregorodtsev@linguanet.ru

Anatoliy V. Tsaregorodtsev, Dr.Sci. (Technical), Professor, Vice-rector for development and IT, Moscow State Linguistic University, Moscow, Russian Federation

Романовский Сергей Валерьевич, директор института информационных наук, ФГБОУ ВО МГЛУ, Москва, Российская Федерация,
e-mail: s.v.romanovskiy@linguanet.ru

Sergey V. Romanovskiy, Director of information sciences Institute, Moscow State Linguistic University, Moscow, Russian Federation

Волков Сергей Дмитриевич, аспирант кафедры международной информационной безопасности, наук, ФГБОУ ВО МГЛУ, Москва, Российская Федерация,
e-mail: volkov1234@gmail.com

Sergey D. Volkov, Postgraduate student of international information security department, Moscow State Linguistic University, Moscow, Russian Federation

Самойлов Вячеслав Евгеньевич, кандидат технических наук, заведующий лабораторией сетей и систем передачи информации, ФГБОУ ВО МГЛУ, Москва, Российская Федерация,
e-mail: v.samoilov@linguanet.ru
ORCID: 0000-0003-3996-6411

Vyacheslav E. Samoilov, Ph.D (Technical), the head of the laboratory of networks and information transmission systems, Moscow State Linguistic University, Moscow, Russian Federation