ОСОБЕННОСТИ И МЕХАНИЗМ ИЗМЕРЕНИЯ И ОБРАБОТКИ РИСКОВ ПРИ ОЦЕНКЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕСА КОМПАНИИ

Т.Ю. Салютина, *зав. кафедрой «Экономика связи», д.э.н., профессор, МТУСИ, 111024, Москва, ул. Авиамоторная 8А, salutina@list.ru;*
М.А. Аблогин, *аспирант, МТУСИ, 111024, Москва, ул. Авиамоторная 8А;*
Г.П. Платунина, *ассистент кафедры «Экономика связи» МТУСИ, 111024, г. Москва, ул. Авиамоторная, 8А, platunina111@gmail.com*

УДК 338.27

Аннотация. Развитие информационного общества сопровождается увеличением рисков вследствие уязвимости ресурсов. Организация работ по управлению и обработке рисков дает возможность компании осуществлять экономически обоснованный выбор мер и средств защиты в информационной системе. В статье рассмотрены особенности измерения рисков и определена модель оценки эффективности системы информационной безопасности бизнеса компании.

Ключевые слова: информационная безопасность; информационные угрозы бизнеса; управление рисками; оценка рисков; защита информации; методика оценки рисков.

FEATURES AND MECHANISM OF MEASURING AND PROCESSING RISKS WHEN ESTIMATING THE EFFICIENCY OF THE BUSINESS INFORMATION SECURITY SYSTEM OF THE COMPANY

Tatiana Salutina, *head of the «Communications economics» department, doctor of economics, professor MTUCI, 111024, Moscow, ul. Aviamotornaya 8A;*
Mstislav Ablogin, *graduate student MTUCI, 111024, Moscow, ul. Aviamotornaya 8A;*
Galina Platunina, *assistant of the «Economic sciences» department MTUCI, 111024, Moscow, ul. Aviamotornaya 8A.*

Annotation. The development of the information society is accompanied by an increase in risks due to the vulnerability of resources. The organization of work to manage and process risks enables the company to make an economically sound choice of measures and protections in the information system. The article discusses the features of risk measurement and defines a model for evaluating the effectiveness of the company's information security system.

Keywords: information security; information threats to business; risk management; risk assessment; information protection; risk assessment methodology.

Компании, бизнес которых во многом зависит от качества информационной инфраструктуры, для достижения целей бизнеса должны поддерживать на необходимом уровне систему обеспечения информационной безопасности. Информационная безопасность представляет собой совокупность аппаратно-программных, технических и организационных защитных мер, функционирующих под управлением информационной безопасности и процессов осознания ИБ, инициирующих и поддерживающих деятельность по менеджменту информационной безопасности [1, 2, 5, 11].

Желание иметь информационную безопасность, адекватную целям информационной безопасности компании по обеспечению доступности, целостности и конфиденциальности информационных активов, приводит к стремлению совершенствовать информационную безопасность компании возможно при условии знания состояния характеристик и параметров используемых защитных мер, менеджмента, информационной безопасности компании и понимания степени их соответствия требуемым характеристикам [13]. Оценить данные

аспекты информационной безопасности компании можно только по результатам ее оценки, полученной с помощью модели оценки информационной безопасности на основании показателей, критериев и с учетом контекста оценки.

Критерии оценки – это все то, что позволяет установить значения оценки для объекта оценки. В качестве критериев оценки информационной безопасности могут использоваться требования, процедуры, и сочетание требований и процедур информационной безопасности, уровень инвестиций, затрат на информационную безопасность [11].

К показателям оценки информационной безопасности компании относятся записи, изложение фактов или любая информация, которая имеет отношение к критериям оценки ИБ и может быть проверена. Такими показателями (свидетельствами) оценки информационной безопасности могут быть доказательства выполняемой и выполненной деятельности по обеспечению ИБ в виде отчетных, нормативных, распорядительных документов, результатов опросов и наблюдений [1, 2, 5].

Контекст оценки информационной безопасности компании объединяет цели и назначение оценки ИБ, вид оценки (независимая оценка, самооценка), объект и области оценки ИБ, ограничения оценки и роли [5, 11].

Модель оценки информационной безопасности компании определяет сферу оценки, отражающую контекст оценки информационной безопасности в рамках критерия оценки ИБ, отображение и преобразование оценки в параметры объекта оценки, а также устанавливает показатели, обеспечивающие оценку информационной безопасности [14].

В общем виде процесс проведения оценки информационной безопасности компании (рис. 1) представлен основными компонентами: контекст, свидетельства, критерии и модель оценки – необходимыми для реализации процесса оценки [11].

Оценка информационной безопасности компании заключается в выработке оценочного суждения относительно пригодности (зрелости) процессов обеспечения информационной безопасности, адекватности используемых защитных мер или целесообразности (достаточности) инвестиций (затрат) для обеспечения необходимого уровня информационной безопасности на основе измерения и оценивания критических элементов (факторов) объекта оценки [9].

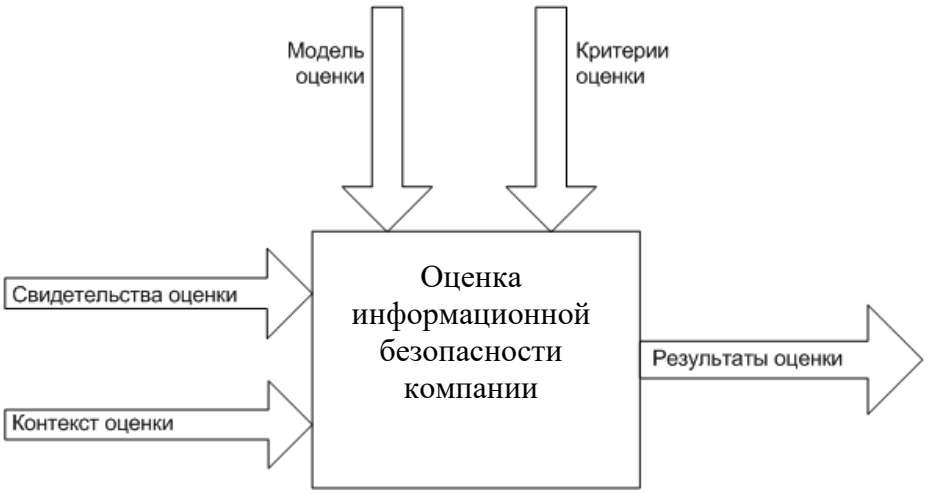

Рисунок 1

Наряду с важнейшим назначением оценки информационной безопасности – создание информационной потребности для совершенствования информационной безопасности (ИБ) компании, возможны и другие цели проведения оценки информационной безопасности, такие как:

- определение степени соответствия установленным критериям отдельных областей обеспечения ИБ, процессов обеспечения ИБ, защитных мер;
- выявление влияния критических элементов (факторов) и их сочетания на ИБ организации;
- сравнение зрелости различных процессов обеспечения ИБ и сравнение степени соответствия различных защитных мер установленным требованиям.

Результаты оценки информационной безопасности компании могут также использоваться заинтересованной стороной для сравнения уровня ИБ организаций с одинаковым бизнесом и сопоставимым масштабом [12].

В зависимости от выбранного для оценки ИБ компании критерия можно разделить способы оценки ИБ компании (рис. 2) на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям (критериям) [11].

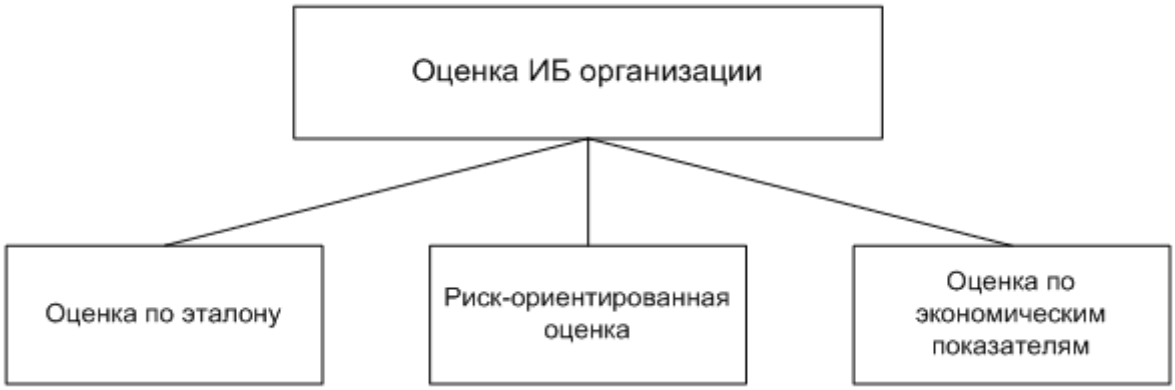

Рисунок 2

Способ оценки ИБ компании по эталону сводится к сравнению деятельности и мер по обеспечению ИБ компании с требованиями, закрепленными в эталоне. По сути дела, проводится оценка соответствия ИБ компании установленному эталону. Под оценкой соответствия ИБ компании установленным критериям понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований ИБ в компании. С помощью оценки соответствия ИБ измеряется правильность реализации процессов системы обеспечения ИБ компании и идентифицируются недостатки такой реализации [11].

В результате проведения оценки информационной безопасности бизнеса компании должна быть сформирована оценка степени соответствия ИБ эталону, в качестве которого могут быть приняты (в совокупности и отдельно):

- требования законодательства Российской Федерации в области информационной безопасности;
- отраслевые требования по обеспечению информационной безопасности;
- требования нормативных, методических и организационно-распорядительных документов по обеспечению информационной безопасности;
- требования национальных и международных стандартов в области информационной безопасности.

Основные этапы оценки информационной безопасности по эталону включают выбор эталона и формирование на его основе критериев оценки информационной безопасности, сбор свидетельств оценки и измерение критических элементов (факторов) объекта оценки, формирование оценки информационной безопасности компании [16].

Риск-ориентированная оценка информационной безопасности компании представляет собой способ оценки, при котором рассматриваются риски информационной безопасности,

возникающие в информационной сфере компании, и сопоставляются существующие риски информационной безопасности и принимаемые меры по их обработке. В результате должна быть сформирована оценка способности компании эффективно управлять рисками информационной безопасности для достижения эффективности и устойчивости бизнеса компании [17].

Основные этапы риск-ориентированной оценки информационной безопасности включают идентификацию рисков информационной безопасности, определение адекватных процессов менеджмента рисков и ключевых индикаторов рисков информационной безопасности, формирование на их основе критериев оценки информационной безопасности, сбор свидетельств оценки и измерение риск-факторов, формирование оценки информационной безопасности компании [15].

Способ оценки информационной безопасности компании на основе экономических показателей оперирует понятными для бизнеса аргументами о необходимости обеспечения и совершенствования информационной безопасности компании. Для проведения оценки в качестве критериев эффективности ИБ компании используются показатели совокупной стоимости владения (*Total Cost of Ownership – TCO*) [2].

Под показателем *TCO* понимается сумма прямых и косвенных затрат на внедрение, эксплуатацию и сопровождение системы обеспечения информационной безопасности. Под прямыми затратами понимаются все материальные затраты, такие как покупка оборудования и программного обеспечения, трудозатраты соответствующих категорий сотрудников. Косвенными являются все затраты на обслуживание системы обеспечения информационной безопасности, а также потери от произошедших инцидентов. Сбор и анализ статистики по структуре прямых и косвенных затрат проводится, как правило, в течение года. Полученные данные оцениваются по ряду критериев с показателями ТСО аналогичных компаний отрасли.

Оценка на основе показателя *TCO* позволяет оценить затраты на информационную безопасность и сравнить ИБ компании с типовым профилем защиты, а также управлять затратами для достижения требуемого уровня защищенности [15].

Основные этапы оценки эффективности системы обеспечения информационной безопасности (СОИБ) на основе модели *TCO* включают сбор данных о текущем уровне *TCO*, анализ областей обеспечения ИБ, выбор сравнимой модели *TCO* в качестве критерия оценки, сравнение показателей с критерием оценки, формирование оценки ИБ компании.

Однако этот способ оценки требует создания общей информационной базы данных об эффективности СОИБ компаний схожего бизнеса и постоянной поддержки базы данных в актуальном состоянии. Такое информационное взаимодействие компаний, как правило, не соответствует целям бизнеса. Поэтому оценка ИБ компаний на основе показателя *TCO* практически не применяется.

Риск-ориентированная оценка информационной безопасности бизнеса компании позволяет получить достоверную информацию о состоянии системы информационной безопасности бизнеса компании. Оценка, основанная на измерении риска и управлении риском, отличается от системно-ориентированной и процессно-ориентированной оценки и называется [10] риск-ориентированной оценкой. Ключевое отличие риск-ориентированной оценки заключается в том, что оценка должна быть направлена на анализ того, как менеджмент организации оценивает риски, контролирует и проверяет процессы менеджмента риска [3, 7, 9, 11].

Риск-ориентированная оценка дает объективное и наиболее информативное представление об уровне эффективности деятельности организации, эффективности принимаемых менеджментом решений и эффективности затрат на поддержание и развитие ИБ бизнеса, исходя из сопоставления существующих рисков и принимаемых компанией мер по обработке возможных рисков ИБ бизнеса компании [19].

Целью риск-ориентированной оценки ИБ бизнеса компании является определение того, что:

- процесс оценки менеджмента рисками должным образом создан и внедрен в систему менеджмента;
- процесс менеджмента рисками действует надлежащим образом;
- в отношении рисков, подлежащих обработке, действия менеджмента направлены на снижение этих рисков до приемлемого уровня.

Алгоритм проведения риск-ориентированной оценки показан на рис. 3.
При проведении риск-ориентированной оценки ИБ бизнеса компании следует:

- оценить инфраструктуру менеджмента рисков (ресурсов, документации, методов, сообщения);
- оценить специфические риски;
- при необходимости пересматривать бизнес-цели и процессы менеджмента рисков ИБ бизнеса компании;
- конечный результат оценки рисков ИБ компании должен заключаться в обеспечении уверенности в том, что менеджмент оценки рисков осуществляется надлежащим образом и направлен на снижение рисков до приемлемого уровня.

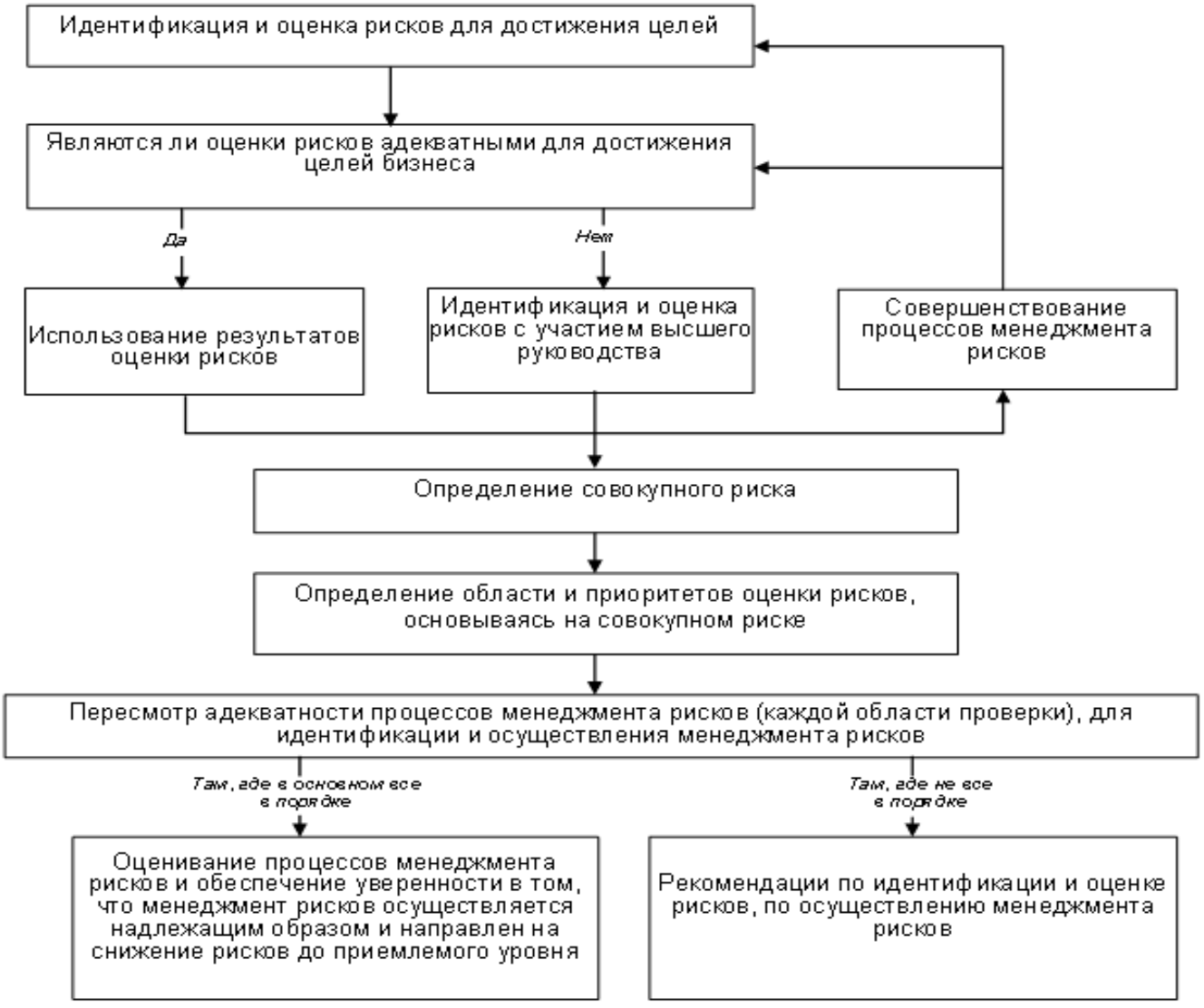

Рисунок 3

На рис. 4 показана модель риск-ориентированной оценки ИБ бизнеса компании.

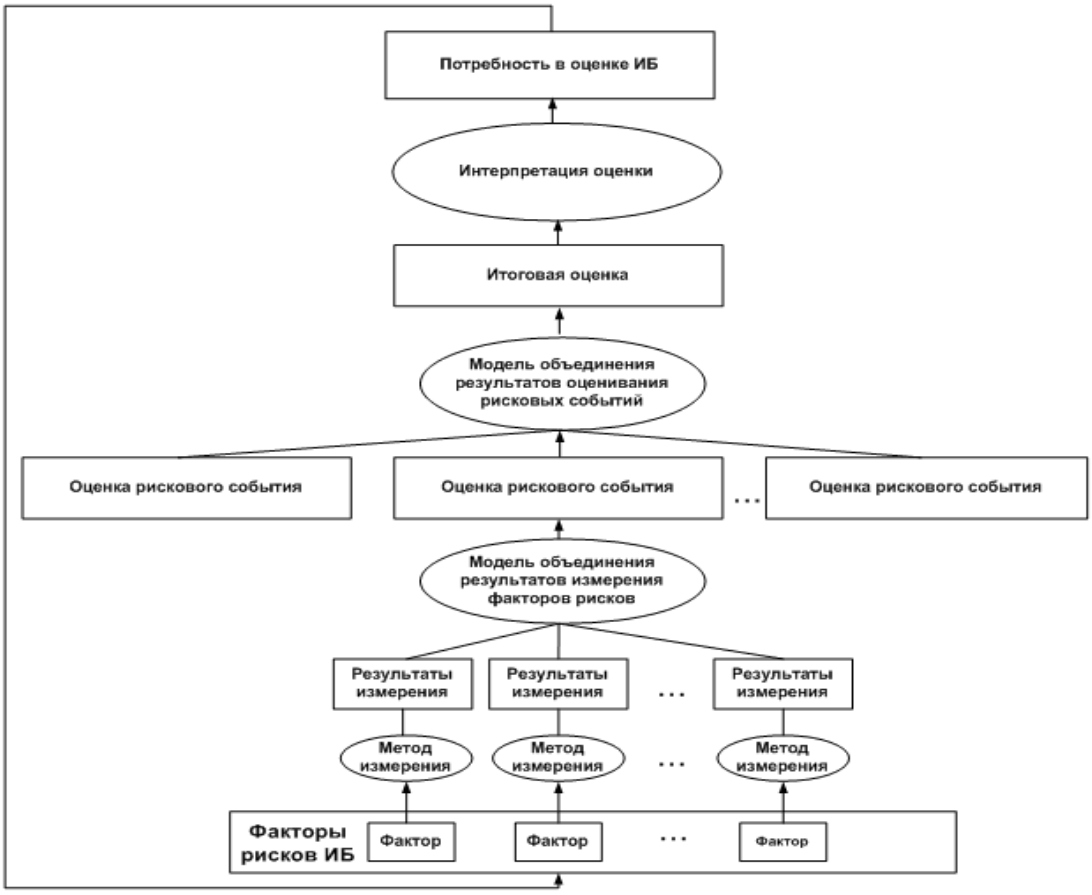

Рисунок 4

Риск реализуется через рисковые события, создающие ущерб целям бизнеса. В свою очередь, рисковые события являются следствием сочетания факторов риска, т.е. любому рисковому событию соответствует некоторый набор факторов риска [11, 18].

Измерить фактор риска – это значит установить степень соответствия состояния *r* фактора риска некоторому состоянию *rm*, определяющему проявление рискового события.

Для совокупности факторов риска функция соответствия:

$$r = r(R, Rm)$$

показывает степень достижения состояний *R* факторов риска нежелательных состояний *Rm* (состояний проявления рискового события).

Для каждого фактора риска, когда *R* и *Rm* являются неслучайными (детерминированными) переменными, функция соответствия служит результатом *Wij* измерения, полученного с помощью выбранного метода измерения:

$$Wij = r(rij, rmij),$$

где:
i – количество оцениваемых рисковых событий, *j* – количество факторов риска *i*-го рискового события.

Объединение результатов измерения факторов риска с целью оценивания совокупности факторов риска может быть реализовано на основании модели предпочтения на множестве факторов риска, относящихся к каждому рисковому событию. Такой же подход может применяться и для формирования итоговой оценки, определяющей совокупный риск ИБ компании [20].

Риск-ориентированная оценка рисков информационной безопасности (ИБ) бизнеса компании позволяет существенно повысить качество менеджмента компании и обеспечить устойчивость и безопасность бизнеса.

Литература

1. ISO/IEC 27004, Information technology – Security techniques – Information security management – Measurement.
2. Gartner. The Price of Information Security. Strategic Analysis Report
3. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. –М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
4. СТО БР ИББС-1.0-2008 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.
5. СТО БР ИББС-1.1-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности
6. BSI PAS 56 Guide to Business Continuity Management (BCM).
7. ISO/IEC 15504 Information technology – Process assessment.
8. NIST Special Publication 800-55 «Security Metrics Guide for Information Technology Systems.
9. Зефиров С.Л., Голованов В.Б. Как измерить информационную безопасность организации? Объективно о субъективном // Защита информации. Инсайд, 2016. – № 3.
10. Институт «внутренних» аудиторов – Великобритания и Ирландия // Проведение риск-ориентированного внутреннего аудита, 2017.
11. Оценка информационной безопасности бизнеса. В.В. Андрианов, В.Б. Голованов, Н.А. Голдуев, С.Л. Зефиров, 2016.
12. Салютина Т.Ю., Володина Е.Е., Кухаренко Е.Г. Стратегическое управление развитием инфокоммуникационных компаний // Экономика и качество систем связи, 2018. – № 1 (7). – С. 3-11.
13. Кухаренко Е.Г., Салютина М.Е. Применение методов стратегического анализа для оценки конкурентоспособности телекоммуникационных компаний // T-Comm: Телекоммуникации и транспорт, 2014. – Т. 8. – № 7. – С. 57-59.
14. Салютина Т.Ю., Ромашин А.А. Анализ моделей управления бизнес-процессами компаний связи T-Comm: Телекоммуникации и транспорт, 2012. – Т. 6. – № 12. – С. 90-93.
15. Салютина Т.Ю., Платунина Г.П., Цыкалова М.Е. Проблемы измерения и обработки рисков при оценке эффективности системы информационной безопасности бизнеса предприятия // Технологии информационного общества сборник трудов XII Международной Отраслевой Научно-Технической конференции, 2018. – С. 360-363.
16. Салютина Т.Ю. Инструментарий оценки качества корпоративного управления в интегрированной модели инвестиционной привлекательности телекоммуникационных компаний //Экономика и качество систем связи, 2016. – № 2. – С. 27-34.
17. Салютина Т.Ю., Кузовков А.Д. Управление инновационным развитием инфокоммуникаций на основе оценки эффективности применения ИКТ // Экономика и качество систем связи, 2017. – № 2 (4). – С. 3-8.
18. Салютина Т.Ю., Щекотова Е.В. Роль стратегического планирования в реализации рыночного потенциала операторов связи. Труды Московского технического университета связи и информатики (см. в книгах), 2009. – Т. 12. – С. 12.
19. Салютина Т.Ю., Щекотова Е.В. Методические основы оценки эффективности бизнеса телекоммуникационных компаний на основе сбалансированной системы показателей. В книге:

Технологии информационного общества Тезисы докладов московской отраслевой научно-технической конференции, 2007. – С. 211-212.
20. Салютина Т.Ю., Платонова Н.С. Проблема комплексного учета рисков при оценке эффективности инвестиционных проектов // в книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом сборник материалов (тезисов) XXXVIII международной конференции РАЕН. 2016. – С. 28-29.