Научно-технические ведомости СПбГПУ. Экономические науки. 2021, Том 14, № 6. С. 102–116.
St. Petersburg State Polytechnical University Journal. Economics. 2021, Vol. 14, No. 6. Pp. 102–116.

Научная статья
УДК 338.27
DOI: https://doi.org/10.18721/JE.14608

ОЦЕНКА КИБЕРРИСКОВ В ПРОЕКТАХ ИНТЕРНЕТА ВЕЩЕЙ

С.В. Гришунин , И.Ю. Пищалкина ✉ , С.Б. Сулоева

Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, Российская Федерация

✉ eskelinen.ilona@gmail.com

Аннотация. Интернет вещей (IoT) открывает широкие возможности для инноваций, начиная от промышленных предприятий до здравоохранения и потребителей. Однако развитие проектов Интернета вещей создает значительные риски для разработчиков и пользователей. Количество и частота IoT-атак увеличивается и наблюдается рост прямого и косвенного ущерба. Так одно зараженное устройство может открыть для атаки всю экосистему компании с потенциальными сбоями: от нарушения конфиденциальности отдельных пользователей до массового сбоя общественных систем и угрозы для жизни людей. Актуальность выбранной темы объясняется ростом числа кибератак, скоростью появления новых угроз и увеличением ущерба от атак. Поэтому в статье рассматривается снижение эффективности существующих механизмов оценки киберрисков и восполняются пробелы в исследованиях в этой области. Авторами был разработан показатель Cyber ROI (CyROI), позволяющий отразить киберриски и измерить эффективность инвестиций в развитие Интернета вещей с учетом киберпреступности и связанных с ним мер контроля. Далее был сформирован подход к оценке киберрисков для проектов Интернета вещей (IoT), основанный на принципах риск-контроллинга и включающий этапы выявления рисков, моделирования деревьев рисков, оценки рисков и анализа результатов. Помимо формирования самого подхода, была представлена структурно-логическая схема оценки киберрисков и описаны входящие в него инструменты. В отличие от аналогов, разработанный подход обеспечивает системность в оценке киберрисков; позволяет интегрировать и координировать все связанные с этим действия и инструменты, моделировать доверительный интервал возможной рентабельности инвестиций, а также показывает шансы выйти за рамки риск-аппетита и толерантности к риску. Предложенный подход делает оценку киберрисков динамичной, итеративной, реагирующей на изменения в киберсреде. Также данный подход имеет значительное научное и практическое применение. По сравнению с существующими подходами, предложенный авторами подход к оценке киберрисков обладает большей гибкостью, учитывает корреляции между рисками, позволяет оценить влияние каждого фактора риска на CyROI и рассчитывать большое количество сценариев.

Ключевые слова: интернет вещей, киберриски, кибербезопасность, риск-контроллинг

Для цитирования: Гришунин С.В., Пищалкина И.Ю., Сулоева С.Б. Оценка киберрисков в проектах интернета вещей // Научно-технические ведомости СПбГПУ. Экономические науки. 2021. Т. 14, № 6. С. 102–116. DOI: https://doi.org/10.18721/JE.14608

Scientific article
DOI: https://doi.org/10.18721/JE.14608

ASSESSING CYBER RISKS IN THE INTERNET OF THINGS PROJECTS

S.V. Grishunin , I.Yu. Pishchalkina ✉ , S.B. Suloeva

Peter the Great St. Petersburg Polytechnic University,
St. Petersburg, Russian Federation

✉ eskelinen.ilona@gmail.com

Abstract. The Internet of Things (IoT) opens up vast opportunities for innovation, ranging from industrial enterprises to healthcare and consumers. However, the development of Internet of Things projects creates significant risks for developers and users. The number and frequency of IoT attacks is increasing, while the direct and indirect damage are on the rise. Thus, one infected device can make the entire ecosystem of a company vulnerable to attacks with potential failures: from violating the privacy of individual users to a massive failure of public systems and a threat to people's lives. The relevance of the article is explained by the increase in the number of cyber attacks, the speed of the emergence of new threats and the increase in damage from attacks. Therefore, the article examines the decrease in the effectiveness of the existing mechanisms for assessing cyber risks and fills the gaps in research in this area. The authors developed Cyber ROI indicator (CyROI), which allows reflecting cyber risks and measuring the effectiveness of investments in the development of the Internet of Things, taking into account cybercrime and related control measures. Next, an approach to cyber risk assessment for Internet of Things (IoT) projects was formed, based on the principles of risk controlling and including the stages of risk identification, risk tree modeling, risk assessment and analysis of results. In addition to the formation of the approach itself, a structural and logical scheme for assessing cyber risks was presented with its tools described. Unlike analogues, the developed approach provides a holistic approach to the assessment of cyber risks; it allows integrating and coordinating all related actions and tools, simulating the confidence interval of possible return on investment, and shows the chances to go beyond risk appetite and risk tolerance. The proposed approach makes the assessment of cyber risks dynamic, iterative, responsive to changes in the cyber environment. Moreover, this approach has significant scientific and practical application. Compared to existing approaches, the author's approach to cyber risk assessment has more flexibility, takes into account correlations between risks, allows you to assess the impact of each risk factor on CyROI and calculate a large number of scenarios.

Keywords: internet of things, cyber risks, cybersecurity, risk controlling

Citation: S.V. Grishunin, I.Yu. Pishchalkina, S.B. Suloeva, Assessing cyber risks in the internet of things projects, St. Petersburg State Polytechnical University Journal. Economics, 14 (6) (2021) 102–116. DOI: https://doi.org/10.18721/JE.14608

Введение

Интернет вещей (IoT) – это набор технологий и приложений, которыми оснащают устройства для генерации данных и информации, с возможностью подключения этих устройств для мгновенного анализа данных и, в идеале, «умных» операций с ними [1]. Технология Интернета вещей позволяет физическим объектам использовать интернет для передачи данных об их состоянии, положении или других атрибутах. В IoT информационные и коммуникационные технологии слились воедино и сформировали информационно-коммуникационное пространство [2].

Ожидается, что количество устройств, подключенных к IoT, будет расти совокупными годовыми темпами на 15% и достигнет 31 миллиарда единиц к 2020 году при предполагаемой рыночной стоимости в 1,1 триллиона долларов [1]. Данная тенденция сопряжена (1) со снижением цен на пропускную способность, хранение данных и вычислительную технику; (2) растущим исполь-

зованием расширенного интеллекта; (3) и проникновением промышленных роботов. Промышленные устройства Интернета вещей (такие как устройства для мониторинга на основе условий и прогнозного обслуживания основных фондов) будут охватывать около 50% глобальных расходов на Интернет вещей [1]. Устройства для потребителей, здравоохранения или общественных услуг будут занимать долю в размере 25% каждое [1].

Наряду с перечисленными возможностями, данная отрасль характеризуется значительными трудностями, которые могут остановить инвестиции в этот сектор. Они включают (1) отсутствие инфраструктуры для управления устройствами; (2) угроза непринятия устройств пользователями; (3) плохое исполнение поставщиками, (4) проблемы с эксплуатацией; или (5) отсутствие регулирования [1]. Наиболее опасной угрозой является растущее число кибератак на устройства Интернета вещей; одна только киберпреступность обходится странам во всем мире более чем в 1 миллиард долларов [3, 4, 5]. Примеры кибератак включают (1) атаки с распределенным отказом в обслуживании (DDOS); (2) кража данных и личных данных; (3) разведывательные атаки; (4) промежуточное проникновение человека; (5) Трояны и вирусы и другие [6]. Растущая сложность, взаимосвязь и распространенность Интернета вещей подвергают эти устройства новым видам опасностей, для которых существующие методы управления рисками не предназначены, в том числе ни для выявления, ни для прогнозирования [2, 7]. Актуальность исследования обусловлена тем, что эти проблемы вынуждают разработчиков интернета вещей, поставщиков и пользователей пересмотреть подходы к управлению киберрисками [7] и переключиться на новейшие системы, такие как управление рисками проекта [8, 9].

В таких условиях процедуры оценки киберрисков должны быть интегрированы и скоординированы в единый подход, который опирается на комбинацию методов и инструментов, а также обеспечивает диапазон вероятных денежных потерь от киберпреступности в течение определенного периода. Предлагаемый подход к оценке киберрисков должен обеспечивать своевременное выявление и оценку угроз, предвидение вероятных новых угроз, а также разработку и реализацию решений по снижению рисков. Проведенное исследование показывает, что многие существующие подходы, такие как оценка уязвимости активов с точки зрения операционной угрозы (OCTAVE) или киберценности, подверженной риску (CyVAR), лишь частично служат этим целям. Поэтому авторами предложен подход, имитирующий доверительный интервал для целевых значений проекта (ROI) с учетом рисков и показывающий шансы выйти за рамки склонности к риску. Он включает в себя инструменты и методы, позволяющие оценивать частоту рисков с помощью нескольких точек данных, обеспечивает целостный подход к оценке киберрисков, объединяет и координирует все виды деятельности по оценке киберрисков. Это делает оценку киберрисков динамичной, итеративной, реагирующей на изменения в киберсреде.

Литературный обзор

В результате детального анализа отечественных [5] и зарубежных научных исследований [6, 7], авторами было выявлено большое разнообразие подходов к оценке рисков, которые можно разделить на: (1) качественные модели; (2) модели зрелости; (3) стандарты управления рисками; (4) количественные модели. Для последующего анализа этих исследований был применен подход SWOT-анализ (сильные и слабые стороны, возможности и угрозы) [3].

Основными достоинствами качественных моделей, таких как оценка уязвимости активов и угроз с точки зрения эксплуатации (OCTAVE) [10], анализ оценки и устранения угроз (TARA) [11] или анализ режимов и последствий кибератак (CyFMEA) [3, 4], являются (1) целостный подход; (2) простота и низкая стоимость; и (3) применимость для оценки возникающих рисков без или с ограниченной статистикой. Благодаря этим сильным сторонам данные методы применимы к разработчикам Интернета вещей малого и среднего бизнеса. К слабым сторонам, рассмотренных моделей можно отнести: (1) качественную интерпретацию вероятности угрозы и воздействия, а

также точечные оценки; (2) упрощение корреляций между рисками и расчета совокупной экспозиции; и (3) отсутствие связи между воздействием риска и целями проекта [12]. Результирующими угрозами являются несоответствие принятию рисков, сжатие диапазона или смещение центра [13]. Возможности для улучшений включают (1) расширение количественной оценки рисков [14]; или (2) добавление метода нечеткой логики, который позволяет улучшить интеграцию мнений экспертов [15]. Тем не менее, даже этих улучшений окажется недостаточно для элиминации слабых сторон.

Сильные стороны моделей зрелости управления рисками (RMM), таких как интегрированная модель зрелости возможностей (CMMI) или Exostar [3], обеспечивают оценку зрелости системы управления киберрисками Интернета вещей по сравнению со стандартами управления рисками с выявлением пробелов. Их недостатком является сосредоточение внимания на выявлении уязвимостей без оценки масштабов воздействия в слабых местах и влияния на цели проекта. Возможность для RMMS заключается в интеграции с другими подходами.

Сильные стороны стандартов информационной безопасности, таких как ISO 27001:2013 [16] или NIST [17], заключаются в том, что они (1) являются проверяемыми и широко признанными международными стандартами в области кибербезопасности; и (2) обеспечивают целостную основу для организации управления киберрисками [3, 16]. Однако они не предоставляют (1) подробных моделей и инструментов для оценки рисков; и (2) информацию для руководства, так как эти модели могут быть интегрированы и применены при принятии решений, ориентированных на риски.

Наконец, стохастические количественные модели (SQM), такие как cyber value at risk (CyVAR), используют теорию вероятностей для оценки доверительного интервала вероятных потерь от киберпреступности в течение данного периода времени [3]. Сильные стороны SQM заключаются в том, что данные модели обеспечивают количественную оценку потерь при моделировании очень большого числа сценариев. Ограничения данного подхода к оценке рисков [3, 6] заключаются в том, что они (1) обеспечивают только инструмент оценки рисков, но не целостный подход к оценке рисков; (2) редко получают доступ к влиянию потерь на целевые показатели проекта; (3) могут привести к угрозам игнорирования возникающих рисков из-за отсутствия данных [3]. Возможность SQMs заключается в разработке полномасштабных подходов к управлению и оценке киберрисков.

Подводя итог, можно сказать, что существующие подходы к оценке рисков в киберпространстве ограничены рядом критических ограничений. Предложенный авторами подход позволит нивелировать пробелы в исследованиях путем разработки подхода к оценке киберрисков в инвестиционных проектах Интернета вещей, основанного на принципах риск-контроллинга. Следовательно, *объектом исследования* выступают инвестиционные проекты, направленные на развитие Интернета вещей, а *предметом* – методический подход к оценке киберрисков для проектов Интернета вещей, построенный на принципах риск-контроллинга.

Целью исследования является формирование усовершенствованного целостного подхода к оценке киберрисков в проектах Интернета вещей. В соответствии с заданной целью поставлены следующие научно-исследовательские *задачи*: 1) формирование концепции подхода к оценке киберрисков; 2) разработка структурно-логической схемы оценки киберрисков и описание этапов оценки; 3) проведение сравнительного анализа, предложенного и существующих подходов, с выделением отличительных особенностей, преимуществ и специфических условий функционирования.

Методы исследования

Методологической базой исследования выступают существующие системы оценки киберрисков, в том числе качественные и количественные методы оценки рисков, стандарты управления

рисками и модели зрелости, как было описано ранее. Также, авторами в рамках формирования подхода к оценке киберрисков в проектах по развитию Интернета вещей, были проанализированы концептуальные положения риск-контроллинга [8, 9, 18].

В ходе исследования были рассмотрены и использованы существующие методы качественной (OCTAVE, TARA) и количественной оценки рисков (SQM, VAR), точечные оценки среднего риска (FMEA или карты рисков), модели зрелости управления рисками (RMM), соответствующие действующие стандарты и применены методы имитационного моделирования (Монте-Карло, PERT).

Результаты и их обсуждение

Риск контроллинг (РК) – это целенаправленный набор методов, процессов и инструментов, направленных на идентификацию и анализ рисков и возможностей, влияющих на достижение стратегических целей компании, а также принятие оптимальных управленческих мер по нейтрализации угроз и использованию возможностей [9, 18]. РК обеспечивает архитектуру (инфраструктуру и процессы) управления рисками. Применяя эту инфраструктуру к конкретным рискам, руководители проектов принимают решения, основанные на оценке рисков. Функции РК перечислены в [18]. Преимущества РК по сравнению с широко применяемым интегрированным управлением рисками заключаются в (1) содействии управлению рисками; (2) интеграции управления рисками в процесс принятия решений на всех этапах проекта; (3) координации всех мероприятий по управлению рисками; и (4) применении инструментов с низкой устойчивостью к риску и повышенным вниманием к количественной оценке рисков [8, 18].

В области кибербезопасности РК направлен на снижение риска того, что пользователи IoT-решения не смогут достичь целевого показателя рентабельности инвестиций (ROI) из-за потерь от киберпреступности [9]. Чем сложнее проект интернета вещей, тем больше может быть разрыв между реальной и целевой рентабельностью инвестиций (рис. 1).

Описанная закономерность подкрепляется (1) ростом привлекательности IoT-устройств для злоумышленников с увеличением масштаба; и (2) растущей изощренностью атак, приводящей к увеличению затрат на контроль и исправление [19]. Чтобы отразить киберриски, авторами был разработан показатель Cyber ROI (CyROI), который измеряет эффективность инвестиций в развитие Интернета вещей с учетом киберпреступности и связанных с ним мер контроля.

$$CyROI = \frac{\left(B - CL \times ME - C_{cs}\right) - I_{IoT} - I_s}{I_{IoT} + I_s},$$

где B – выгоды клиента от применения устройства Интернета вещей; CL – убытки от киберпреступности; ME – коэффициент смягчения последствий, учитывающий решение для обеспечения кибербезопасности; I_{IoT} – инвестиции клиента в IoT-устройства; I_s – инвестиции клиента в разработку решения для обеспечения кибербезопасности; C_{cs} – затраты на обслуживание решения для обеспечения кибербезопасности.

Чтобы сократить этот разрыв, разработчикам Интернета вещей необходимо оптимизировать взаимосвязь между выгодами от внедрения технологии; (2) остаточными потерями от кибератак с учетом системы управления; и (3) инвестициями в системы контроля и устранения киберугроз (решения по кибербезопасности (CS)). В риск-контроллинге эта оптимизация выполняется путем внедрения в IoT экономически эффективной системы управления. Такая система должна (1) предотвращать и предвидеть угрозы до их возникновения; (2) отслеживать и нейтрализовывать уже действующие риски; и (3) как можно быстрее восстанавливать нормальную работу, если произошло рисковое событие [9, 19, 20]. Важнейшим вопросом для разработчика

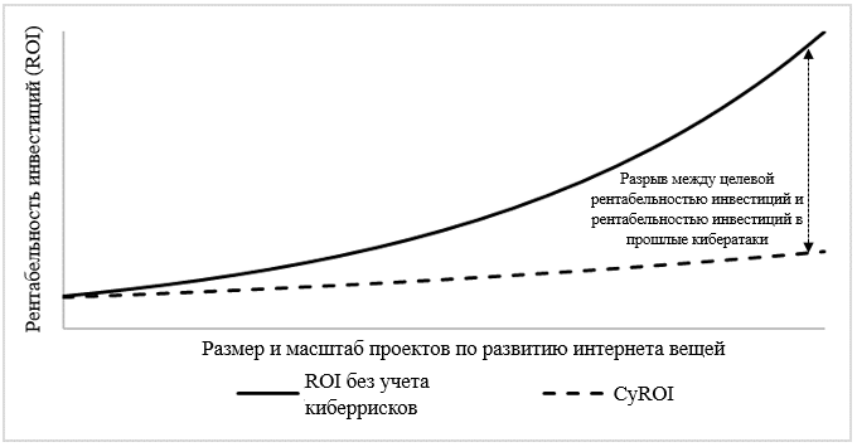

Рис. 1. Влияние кибератак на рентабельность IoT-проектов
Fig. 1. Impact of cyber-attacks on IoT project ROI
Источник. Составлено авторами

Интернета вещей является точная оценка потенциального влияния угрозы на рентабельность инвестиций проекта, чтобы принять решение о экономически эффективных мерах и методах минимизации ее последствий.

Разработанная авторами структурно-логическая схема оценки киберрисков представлена на рис. 2. Предпосылкой для применения данного подхода к оценке является система контроля киберрисков в проектной компании. Такая система может быть построена на основе стандарта ISO 27000 или NIST [3, 17]. Кроме того, требуется четкое понимание бизнес-факторов компании, соображений безопасности, а также правовых, нормативных и договорных требований, специфичных для использования конкретной технологии Интернета вещей.

Первыми входными данными структурно-логической схемы являются бизнес-характеристики устройства Интернета вещей, необходимые для дальнейшей оценки критичности и уязвимости и расчета CyROI. Вторым входным параметром является оценка критичности IoT-актива для проектной компании. Для этой цели авторами была применена аддитивно-мультипликативная модель оценки [21]. Модель описывает активы Интернета вещей по критическим факторам в нескольких измерениях. Они оказывают влияние на ключевые бизнес-процессы и операции компании; посторонних лиц (клиентов, поставщиков) и персонал. Другие включают (1) связи и взаимодействие с другими важными информационными активами; (2) прямые и косвенные затраты на сбой технологии IoT (включая деловую репутацию, регулирующее воздействие и влияние на гудвилл); (3) стоимость потери информации и ее восстановления; (4) время и стоимость возврата активов к нормальной работе; и (5) инвестиции в восстановление IoT. Помимо этого, необходимо также учитывать конфиденциальность, целостность и доступность применяемой технологии [16].

После оценки этих измерений рассчитывается итоговый балл (баллы), сравнивается с пороговым значением и принимается решение о признании проекта Интернета вещей в качестве критического актива.

$$S = \sum_{i=1}^{N} w_i \times X_i,$$

где X_i – оценка критического фактора, оцененная экспертами, $I \in [1, N]$, N – количество факторов; w_i – вес i-го фактора.

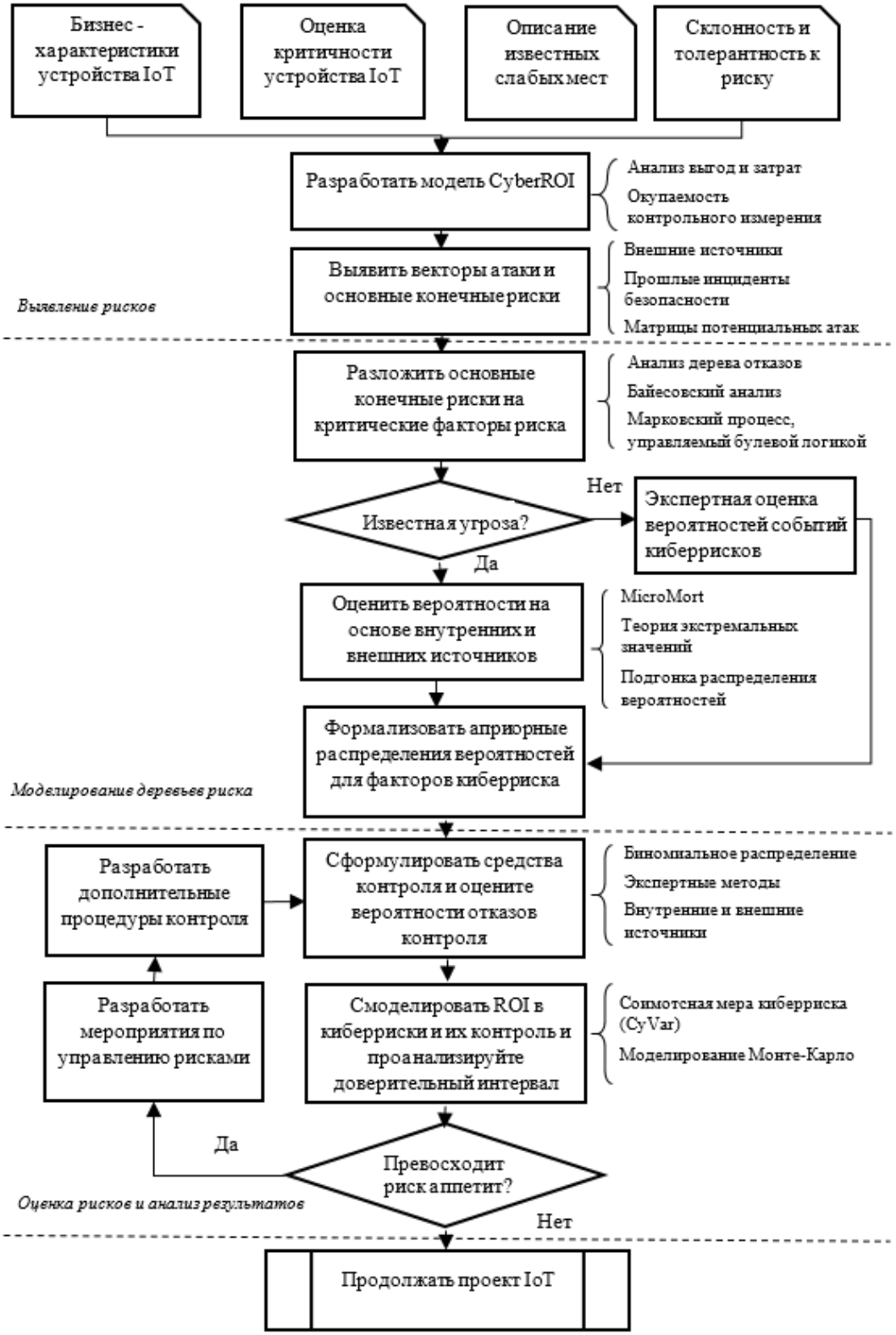

Рис. 2. Структурно-логическая схема оценки киберрисков

Fig. 2. Structural-logical scheme of cyber risk assessment

Источник. Составлено авторами

Второй вход – это результаты оценки уязвимости Интернета вещей. Это делается с использованием удаленного ИТ-управления (RMM), с возможным применением модели зрелости кибербезопасности и программного обеспечения и инструментов для сканирования уязвимостей [3]. Первый подход оценивает зрелость модели кибербезопасности Интернета вещей в соответствии со стандартами [16, 17], позволяя выявить слабые места в системе безопасности в целом и в конкретных областях для сканирования, а также помогает определить области улучшения. Программное обеспечение для сканирования определяет фактические уязвимости в слабых местах и помогает оценить их серьезность.

Последними входными параметрами являются уровень емкости риска (CyROIT) и риск-аппетит (CyROIR). Первый параметр – это терминальный уровень киберриска, который может нести компания, в то время как риск-аппетит – это максимальный уровень киберрисков, который она может принять в ходе достижения целевых показателей. Данные параметры характеризуются вероятностями достижений – γ или δ соответственно. Для рассматриваемого подхода к оценке киберрисков мы устанавливаем γ и δ на уровне 90% и 95% соответственно, но компания может изменить эти пределы.

После сбора всех входных данных модель CyROI разрабатывается с использованием формулы для расчета CyROI и подхода анализа дерева событий [14]. Для определенного IoT-решения (например, система прогнозного технического обслуживания), в табл. 1 представлены примеры составляющих выгод и потерь от киберпреступности, а также возможные средства управления.

Таблица 1. Примеры компонентов CyROI для системы прогнозного технического обслуживания
Table 1. Examples of components of CyROI for predictive maintenance system

Выгоды и экономия (B)	Кибер потери (CL)	Контрольные точки
– Снижение времени простоя оборудования (время и стоимость); – Повышение безопасности и производительности персонала; – Уменьшение выходных дефектов; – Повышение эффективности цепочки поставок; – Улучшенное управление ресурсами; – Экономия от сокращения рабочей силы	– DDoS-атаки; – Атаки на аппартаное оборудование; – Удаленное выполнение кода; – Нарушения и потери данных (прямые и косвенные затраты); – Подмена данных; – Кража интеллектуальных активов (прямые и косвенные затраты); – Эксплуатируемые конфигурации; – Нарушение основных функций системы	– Ограничение доступа и обеспечение безопасной конфигурации; – Ведение журналов аудита; – Защита от вредоносных программ / антивирусы; – Ограничения и контроль портов, протоколов и сервисов; – Защита границ от внешних угроз; – Тесты на проникновение; – Обучение персонала

Источник. Составлено по [14].

На следующем этапе для каждой уязвимости определяются потенциальные векторы атаки и конечные риски. Такой анализ начинается с определения общих векторов привязки. Источниками являются (1) публикации авторитетных организаций, таких как Отчет по расследованиям инцидентов в области информационной безопасности Verizon, отчеты Symantec или FireEye [21]; (2) анализ внутренней базы данных (если таковая имеется) или внешних баз данных о прошлых киберинцидентах: или (3) экспертные знания. Затем общие векторы обрабатываются для конкретного IoT-проекта и формируются матрицы потенциальных атак [21]. Они помогают определить таксономию атаки, включая (1) инициатора (злоумышленника) атаки; (2) классификацию атаки по общим векторам; (3) тип (внутренний, внешний, смешанный) (4) точку вторжения и требуемые привилегии; (5) действия злоумышленника; (6) цель атаки; и (7) цель злоумышленника (отказ в обслуживании, кража данных, отключение устройства, манипуляция денежными средствами и т. д.). Результатом этого анализа является набор конечных рисков $\{R_i\}_{i\in 1,N}$.

Далее на этапе моделирования деревьев рисков и вероятностей факторов риска, каждый конечный риск разбивается на ключевые факторы риска, и для последних определяются распре-

деления вероятностей. Это делается с помощью дерева в виде диаграммы галстука-бабочки [18], которое (1) обеспечивает структурный анализ риска и визуализацию взаимосвязи между риском, его причинами или последствиями; и (2) помогает определить места для контрмер (рис. 3). В правой части диаграммы представлена модель CyROI, разработанная на предыдущем этапе. Левая часть диаграммы представляет собой причинно-следственную сеть, где конечный узел представляет собой конечный риск, верхние узлы представляют наиболее достоверные факторы риска (C_i) и условия для достижения целей злоумышленника, а нижние узлы являются начальными наборами кибератак.

Для построения структурной причинно-следственной сети применяется анализ дерева отказов (FTA) [15]. Его преимуществом является возможность найти набор минимальных сокращений, относящийся к комбинации минимальных факторов риска, возникновение которых приведет к конечному риску [15]. Расчет вероятности конечного риска зависит от вероятностей факторов риска. Это можно определить с помощью построения байесовской сети по формуле:

$$P(C_1 \dots C_M) = \prod_{j=1}^{M} P\left(C_j \middle/ pa\left(C_j\right)\right),$$

где M – количество факторов риска; $P(C_1 \dots CM)$ – совместное распределение вероятностей всех факторов риска и $P(C_j/pa(C_j))$ – условная вероятность j-го фактора риска с учетом факторов C_j.

Для нижнего (предшествующего) фактора риска в дереве определяется функция распределения вероятностей. В редких случаях имеются данные достаточной глубины и продолжительности (3-5 лет), и есть ожидания, что эти угрозы повторятся в будущем. В этом случае для выбора распределения, наилучшим образом описывающего полученные данные, применяется метод подгонки распределения [2]. Наиболее часто, в этом случае, применяются распределения Пуассона, Вейбулла, логнормальные распределения или распределения из теории экстремальных значений.

В большинстве случаев внутренняя информация о прошлых киберсобытиях очень ограничена. Также могут быть использованы данные авторитетных источников (таких как Cybersecurity, Ventures, Kaspersky Lab, Verizon, Symantec и другие), конференций, подрядчиков, поставщиков, клиентов или коллег. В этом случае используется микромортный подход [2] и применяется бета-распределение вероятностей [12].

$$P(X/\alpha,\beta) = \frac{x^{\alpha-1}(1-x)^{\beta-1}}{B(\alpha,\beta)},$$

$$B(\alpha,\beta) = \int_0^1 t^{\alpha-1}(1-t)^{\beta-1}\,dt,$$

где α – количество признаков, в которых характеристики киберугрозы были обнаружены в рассматриваемый период, β – количество признаков, в которых киберугрозы не были обнаружены в рассматриваемый период.

В ситуации «атаки нулевого дня», когда обнаружена новая уязвимость и отсутствуют данные, распределение вероятностей определяется экспертными методами. В этом случае применяется распределение PERT:

$$P(X/a,b,c) = \frac{(x-a)^{\alpha-1}(c-x)^{\beta-1}}{B(\alpha,\beta)(c-a)^{\alpha+\beta-1}},$$

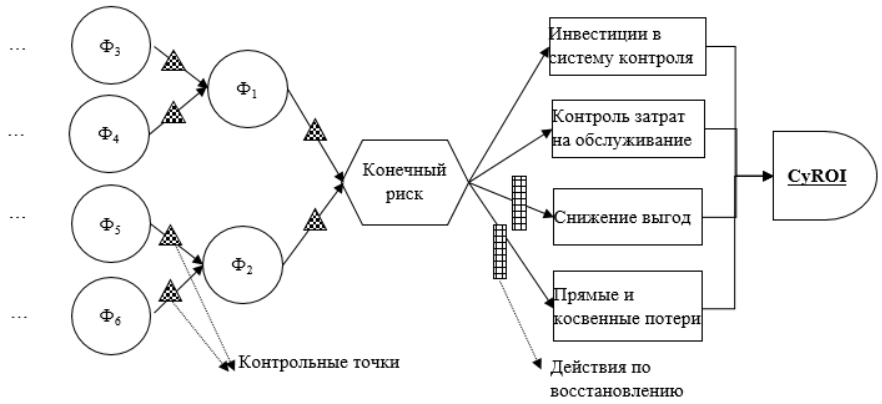

Рис. 3. Диаграмма формирования взаимосвязей факторов риска
с конечным результатом с использованием метода «галстук-бабочка»
Fig. 3. Formation diagram of the relationships between risk factors and the result using the "bow tie" method
Источник. *Составлено по* [22, 23]

$$\alpha = \frac{4b + c - 5a}{c - a},$$
$$\beta = \frac{5c - a - 4b}{c - a},$$

где a, b, c – минимальные (a), наиболее вероятные (b) и максимальные (c) значения, которые могут принимать вероятности.

В случае «атаки нулевого дня» для расчета шансов (a, b, c) «дочернего» фактора риска в дереве с учетом экспертных оценок условных шансов, применяется подход логарифмического отношения шансов (LOR) [12]. LOR не чувствителен к размеру выборки, обеспечивает хорошую интерпретацию переменных и позволяет «суммировать» влияние независимых различных условий на вероятность.

На следующем этапе в дерево добавляются существующие и новые критические элементы управления кибербезопасностью и разрабатываются распределения вероятностей каждого сбоя управления. В случае правильной статистики или треугольного распределения, параметры которого оцениваются экспертами (при отсутствии статистики), распределение Бернулли [12] является наиболее распространенным в этом случае.

На последнем этапе следует установить корреляции между конечными рисками. Они рассчитываются на основе прошлых статистических данных (если таковые имеются) или оцениваются экспертами.

Как только моделирование вероятностных распределений факторов риска завершено и корреляции между конечными рисками определены и смоделированы, моделирование методом Монте-Карло выполняется с помощью генератора псевдослучайных чисел (количество имитаций варьируется от 1000 до 10000 раз). Это моделирование основано на вероятностях и влиянии факторов риска после расчета распределения киберпотерь, таких как:

$$CL_e = P_e * I_e,$$

где CL_e – смоделированные киберпотери, P_e, I_e – смоделированная апостериорная вероятность и влияние риска. После моделирования киберпотерь, моделируется доверительный интервал CyROI в соответствии с моделью, построенной на предыдущем шаге.

Моделирование может быть выполнено в MS Excel с установленным механизмом моделирования @Risk. Результатом моделирования является (1) диапазон возможных значений заданных рисков CyROI; и (2) описательная статистика CyROI (среднее значение, медиана (квантили), дисперсия и стандартное отклонение, мода, доверительные интервалы) и т. д.

Анализ результата включает оценку (1) ожидаемого отклонения CyROI от запланированного ROI; (2) наиболее вероятного значения CyROI; (3) какие конечные риски и факторы риска в наибольшей степени способствовали отклонению результата. Если нижняя граница δ-доверительного интервала CyROI ниже $CyROI_R$, то возможные киберпотери неприемлемы для компании, и проект Интернета вещей следует прекратить или отправить обратно для доработки и устранения узких мест. Если нижняя граница γ-доверительного интервала CyROI выше $CyROI_R$, но ниже $CyROI_T$, то возможные киберпотери превышают уровень, который компания готова нести. Следует ввести дополнительные процедуры контроля, повысить надежность существующего контроля и принять меры по устранению уязвимостей. После принятия этих мер, моделирование методом Монте-Карло выполняется снова, чтобы убедиться, что диапазон возможных значений CyROI находится в пределах границ риска.

Кроме того, анализ результатов помогает определить: (1) какие резервы следует сохранить в случае реализации неблагоприятных сценариев; (2) на каких ключевых областях риска следует сосредоточить внимание главного сотрудника по информационной безопасности (CISO); (3) каковы наиболее оптимистичные и пессимистичные показатели рентабельности инвестиций; и (4) какие планы необходимо разработать на случай непредвиденных обстоятельств при реализации наихудших сценариев.

Таблица 2. Преимущества разработанного подхода перед аналогичными
Table 2. Advantages of the approach over its peers

Сравниваемый подход	Разработанный подход
Качественная оценка рисков (OCTAVE, TARA) или точечные оценки среднего риска (FMEA или карты рисков). Риски описываются с использованием допущений фиксированной стоимости	Система количественной оценки рисков. Факторы риска описываются распределениями вероятностей. Генерирует доверительный интервал значений CyROI на основе большого числа сценариев
Оценка производится только потенциальных убытков от киберрисков без перевода их воздействия на цели проекта	Прогнозирует вероятность достижения целевого ROI проекта с учетом киберрисков
Слабый анализ влияния каждого фактора риска на возможные отклонения ROI	Показывает влияние каждого фактора риска на потенциальные отклонения от CyROI
Ограниченное количество сценариев	Моделирование методом Монте-Карло большого числа сценариев
Не предусматривает шансы выйти за рамки риск-аппетита	Предусматривает шансы выйти за рамки риск-аппетита и толерантности к риску
Трудности расчета совокупных рисков	Вычисляет агрегированные риски с учетом корреляций между рисками
Слабая координация и интеграция процедур оценки рисков и других бизнес-процессов	Интегрирует и координирует все процессы, мероприятия и инструменты оценки киберрисков в рамках риск-контроллинга
Не предусматривает вероятности отказов управления	Предусматривает моделирование вероятности сбоев управления
Требуются данные достаточной глубины и продолжительности для количественной оценки вероятностей	Применяется микромортный подход, позволяющий количественно оценивать вероятности с помощью нескольких точек данных
Предоставляются только инструменты и методы оценки рисков без целостной структуры (CyVAR, карты рисков и регистры)	Обеспечивает целостный подход, начиная от выявления рисков и заканчивая устранением рисков
Представлен только процесс управления рисками без инструментов и методов (ISO 27000 или NIST)	Включает целый перечень инструментов и методов оценки рисков

Источник. Составлено авторами

Таким образом, разработанный авторами подход к оценке киберрисков имеет несколько важных преимуществ перед своими аналогами, такими как RMM, OCTAVE или CyVAR (табл. 2).

По результатам проведенного сравнительного анализа, предложенный подход к оценке киберрисков обладает большей гибкостью и вариативностью, обеспечивает целостный подход, позволяет рассчитывать эффект взаимодополняющих рисков, а также оценивать влияние каждого риска в отдельности на отклонения эффективности инвестиций в развитие Интернета вещей.

Заключение

В рамках данного исследования был разработан подход к оценке киберрисков для проектов Интернета вещей (IoT) для решения проблемы снижения эффективности существующих структур в этой области. Подход имеет преимущества перед существующими аналогами. Он обеспечивает целостную основу для оценки киберрисков; объединяет и координирует все связанные с этим действия. Он содержит эффективные инструменты и методы, позволяющие количественно оценивать кибериски, анализировать их влияние на цель проекта, выстраивать распределение рентабельности инвестиций проекта с учетом рисков и анализировать шансы выхода за рамки склонности к риску. Эти преимущества делают оценку киберрисков динамичной, повторяющейся, реагирующей на изменения в киберсреде и появление новых угроз. Таким образом, проведенное исследование позволило получить следующие основные результаты:

1. Выявлено влияние кибератак на рентабельность IoT-проектов и определено, что с повышением сложности проекта Интернета вещей, может увеличиваться разрыв между реальной и целевой рентабельностью инвестиций;

2. Авторами разработан показатель Cyber ROI (CyROI), позволяющий отразить кибериски и измерить эффективность инвестиций в развитие Интернета вещей с учетом киберпреступности и связанных с ним мер контроля.

3. Далее был разработан подход к оценке киберрисков для проектов Интернета вещей, основанного на принципах риск-контроллинга и включающий этапы (1) выявления рисков; (2) моделирования деревьев рисков; (3) оценки рисков и анализа результатов;

4. Представлена подробная структурно-логическая схема разработанного подхода и рассмотрены примеры компонентов CyROI для системы прогнозного технического обслуживания;

5. Рассмотрены возможности применения к риск-анализу байесовской сети, микромортного подхода, бета-распределения вероятностей, метода Монте-Карло и PERT-распределения.

6. Выявлены основные преимущества подхода к оценке киберрисков перед аналогичными подходами: инструмент обладает большей гибкостью, учитывает корреляции между рисками, позволяет оценить влияние каждого фактора риска на CyROI и рассчитывать большое количество сценариев.

Направления дальнейших исследований

В качестве направлений дальнейших исследований планируется разработка инструментов, таких как (1) подбор соответствующих распределений вероятностей для различных типов киберрисков по имеющимся данным; (2) совершенствование моделей выявления векторов атак и оценки уязвимостей; и (3) разработка передовых моделей калибровки экспертного мнения и оценки вероятностей рисков. Они также включают разработку ключевых индикаторов риска для дальнейшего одновременного контроля рисков.

СПИСОК ИСТОЧНИКОВ

1. Deloitte Inside. The internet of things. A technical primer. Deloitte. 2018. URL: https://www2.deloitte.com/insights/us/en/focus/internet-of-things/technical-primer.html, (accessed: 2019.02.03).

2. **Глухов В.В.** Экономика и менеджмент в инфокоммуникациях: Учебное пособие. Стандарт третьего поколения / В.В. Глухов, Е. Балашова. – Санкт-Петербург: Питер, 2012. – 272 с. – ISBN: 978-5-459-00967-5

3. **Radanliev P., De Roure D.C., Nicolescu R., Huth M., Montalvo R.M., Cannday S., Burnap P.** Future developments in cyber risk assessment for the internet of things. Computers in Industry 102, 14–22 (2018).

4. **Ralston P.A.S., Graham J.H, Hieb J.L.** Cyber security risk assessment for SCADA and DCS networks. ISA Transactions 46, 583–594 (2007).

5. **Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K.** A review of cyber security risk assessment methods for SCADA systems. Computers & Security 56, 1–27 (2016).

6. **Abomhara M., Koien G.** Cyber security and internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security 4, 65–68 (2015).

7. **Nurse S., Greese S., De Roure D.C.** Security risk assessment in internet of things systems, IT Professional 19(5), 20–26 (2017).

8. **Гришунин С.В., Муханова Н.В., Сулоева С.Б.** Разработка концепции риск-контроллинга для промышленного предприятия // Организатор производства. 2018. Т. 26. № 1. С. 45–56. DOI: 10.25065/1810-4894-2018-26-1-45-56

9. **Filko S., Filko I.** Risk controlling of information security. Accounting, analysis and audit: theoretical and practical problems, SSAU 16, 123–127 (2016).

10. **Caralli R., Stevens J., Young L., Wilson W.** Introducing OCTAVE: improving the information security risk assessment process. Hansom AFB, MA (2007).

11. **Wynn J., Whitmore G., Upton L., Spriggs D., McKinnon R., McInnes R., Graubart L., Clausen J.** Threat assessment and remediation analysis (TARA) methodology. Bedford, MA (2011).

12. **Hubbard D., Seiersen R.** How to measure anything in cybersecurity risk. Wiley, NJ (2016).

13. **Thomas P., Bickel J., Bratvold R.** The Risk of Using Risk Matrices. SPE economics and management 6, 56–66 (2013).

14. **Гришунин С.В.** Разработка механизма качественной оценки рисков в стратегическом контроллинге // Научно-технические ведомости СПбГПУ. Экономические науки. 2017. Т. 10. № 2. С. 64–74. DOI: 10.18721/JE.10206

15. **Gusmao A., Poleto T., Silva M., Silva L.** Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. International Journal of Information Management 43 (6), 248–260 (2018).

16. ISO/IEC 27005:2013. Information technology – security techniques – information security risk management. International Organization for Standardization and International Electrotechnical Commission, (2005).

17. Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology (2018).

18. **Grishunin S., Suloeva S., Nekrasova T.** Development of the mechanism of risk-adjusted scheduling and cost budgeting of R&D projects in telecommunications. In: Galinina O., Andreev S., Koucheryavy Y. (eds) NEW2AN ruSMART 2018, LNCS, vol. 11118, pp. 456–470. Springer, Heidelberg (2018).

19. **Antonucci D.** The cyber risk handbook: creating and measuring effective cyber-security capabilities. Wiley Finance, NJ (2017).

20. **Abie H., Balashingham I.** Risk-based adaptive security for smart IoT in e-health. In: Proceedings of the 7th International Conference on Body Area Networks, Oslo, pp. 269–275 (2002).

21. **Kotenko I., Chechulin A.** A cyber attack modeling and impact assessment framework. In: 5th International Conference on Cyber Conflict Proceedings, pp. 1–24. IEEE, Tallinn (2013).

22. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска. – М.: Стандартинформ, 2012. 124 с.

23. **Burova, E., Grishunin, S., Suloeva, S.** (2021). Development of a system-synergetic approach to cost management for a high-tech industrial enterprise. Sustainable Development and Engineering Economics 1, 2.

REFERENCES

1. Deloitte Inside. The internet of things. A technical primer. Deloitte. 2018. URL:https://www2.deloitte.com/insights/us/en/focus/internet-of-things/technical-primer.html, (accessed 2019.02.03).

2. **V. Glukhov, E. Balashova,** Economics and management in info-communication: Tutorial. Piter, SPb (2012).

3. **P. Radanliev, D.C. De Roure, R. Nicolescu, M. Huth, R.M. Montalvo, S. Cannday, P. Burnap,** Future developments in cyber risk assessment for the internet of things. Computers in Industry 102, 14–22 (2018).

4. **P.A.S. Ralston, J.H. Graham, J.L. Hieb,** Cyber security risk assessment for SCADA and DCS networks. ISA Transactions 46, 583–594 (2007).

5. **Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, K. Stoddart,** A review of cyber security risk assessment methods for SCADA systems. Computers & Security 56, 1–27 (2016).

6. **M. Abomhara, G. Koien,** Cyber security and internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security 4, 65–68 (2015).

7. **S. Nurse, S. Greese, D.C. De Roure,** Security risk assessment in internet of things systems, IT Professional 19(5), 20–26 (2017).

8. **S. Grishunin, N. Mukhanova, S. Suloeva,** Development of concept of risk controlling for industrial enterprise. Organizer of Production 26 (1), 45–46 (2018).

9. **S. Filko, I. Filko,** Risk controlling of information security. Accounting, analysis and audit: theoretical and practical problems, SSAU 16, 123–127 (2016).

10. **R. Caralli, J. Stevens, L. Young, W. Wilson,** Introducing OCTAVE: improving the information security risk assessment process. Hansom AFB, MA (2007).

11. **J. Wynn, G. Whitmore, L. Upton, D. Spriggs, R. McKinnon, R. McInnes, L. Graubart, J. Clausen,** Threat assessment and remediation analysis (TARA) methodology. Bedford, MA (2011).

12. **D. Hubbard, R. Seiersen,** How to measure anything in cybersecurity risk. Wiley, NJ (2016).

13. **P. Thomas, J. Bickel, R. Bratvold,** The Risk of Using Risk Matrices. SPE economics and management 6, 56–66 (2013).

14. **S. Grichounine,** Developing the mechanism of qualitative risk assessment in strategic controlling. SPbSPU Journal. Economics 10 (2), 64–74 (2017).

15. **A. Gusmao, T. Poleto, M. Silva, L. Silva,** Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. International Journal of Information Management 43 (6), 248–260 (2018).

16. ISO/IEC 27005:2013. Information technology – security techniques – information security risk management. International Organization for Standardization and International Electrotechnical Commission, (2005).

17. Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology (2018).

18. **S. Grishunin, S. Suloeva, T. Nekrasova,** Development of the mechanism of risk-adjusted scheduling and cost budgeting of R&D projects in telecommunications. In: Galinina O., Andreev S., Koucheryavy Y. (eds) NEW2AN ruSMART 2018, LNCS, vol. 11118, pp. 456–470. Springer, Heidelberg (2018).

19. **D. Antonucci,** The cyber risk handbook: creating and measuring effective cyber-security capabilities. Wiley Finance, NJ (2017).

20. **H. Abie, I. Balashingham,** Risk-based adaptive security for smart IoT in e-health. In: Proceedings of the 7th International Conference on Body Area Networks, Oslo, pp. 269–275 (2002).

21. **I. Kotenko, A. Chechulin,** A cyber attack modeling and impact assessment framework. In: 5th International Conference on Cyber Conflict Proceedings, pp. 1–24. IEEE, Tallinn (2013).

22. GOST R ISO/IEC 31010-2011. Risk management. Methods of risk assessment. – M.: Standartinform, 2012. 124 p.

23. **E. Burova, S. Grishunin, S. Suloeva,** (2021). Development of a system-synergetic approach to cost management for a high-tech industrial enterprise. Sustainable Development and Engineering Economics 1, 2.

СВЕДЕНИЯ ОБ АВТОРАХ / THE AUTHORS

ГРИШУНИН Сергей Вадимович
E-mail: sg279sg279@gmail.com
GRISHUNIN Sergei V.
E-mail: sg279sg279@gmail.com
ORCID: https://orcid.org/0000-0001-5563-5773

ПИЩАЛКИНА Илона Юрьевна
E-mail: eskelinen.ilona@gmail.com
PISHCHALKINA Ilona Yu.
E-mail: eskelinen.ilona@gmail.com

СУЛОЕВА Светлана Борисовна
E-mail: suloeva_sb@mail.ru
SULOEVA Svetlana B.
E-mail: suloeva_sb@mail.ru
ORCID: https://orcid.org/0000-0001-6873-3006

Статья поступила в редакцию 15.10.2021; одобрена после рецензирования 17.12.2021; принята к публикации 17.12.2021.

The article was submitted 15.10.2021; approved after reviewing 17.12.2021; accepted for publication 17.12.2021.