ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ КАК СОСТАВНАЯ ЧАСТЬ СТРАТЕГИЧЕСКОГО КОРПОРАТИВНОГО УПРАВЛЕНИЯ

Шепелёва О.Ю., Шепелёв П.Ю., Газуль С.М.*

Ключевые слова: *информационная безопасность, экономическая эффективность, риск-менеджмент, стратегическое корпоративное управление, информационные системы, модель, факторы, оценки.*

Аннотация.

Цель работы: *изучение современных подходов к оценке эффективности информационной безопасности предприятий малого и среднего бизнеса в России и совершенствование научно-методической базы теории оценки эффективности системы стратегического менеджмента информационной безопасности предприятия для повышения стабильности его функционирования и роста конкурентоспособности на основе использования инновационных методов.*

Метод: *предлагается использовать общенаучные методы, в том числе методы математического моделирования, которые на основе результатов статистического анализа выборки предприятий из базы данных Росстата позволяют разработать модель с наиболее значимыми факторами, влияющими на достоверность оценки информационной безопасности предприятия как составляющей части стратегического корпоративного управления.*

Результаты: *в статье оценка эффективности информационной безопасности рассматривается в качестве основополагающей в системе информационного управления стратегическим развитием современного предприятия. На основе многомерного социотехнического подхода проведена оценка эффективности системы менеджмента информационной безопасности российских предприятий. Результаты показали недостаточное развитие мер, связанных с оптимизацией использования информационных ресурсов и управлением рисками именно на уровне стратегического управления, при наличии у предприятий больших возможностей количественного измерения показателей информационной безопасности. Поэтому авторами была разработана модель, которая рассматривает наиболее значимые факторы, влияющие на достоверность оценки информационной безопасности предприятия малого и среднего бизнеса в России как составляющей части стратегического корпоративного управления, и может быть модифицирована в зависимости от его профиля.*

DOI: 10.21681/1994-1404-2020-4-67-74

Введение

Постоянно растущая скорость внедрения информационных технологий во все сферы жизни современного общества, особенно в условиях, вынуждающих компании переходить на удаленный режим работы (по некоторым оценкам, более половины российских компаний перевели своих сотрудников полностью или частично на удаленный режим работы), тесно связана с вопросами обеспечения информационной безопасности (ИБ).

Поэтому эффективная система менеджмента ИБ компании должна быть направлена на минимизацию рисков реализации бизнес-процессов, рост инвестиций и их рентабельности, обеспечение общего уровня конкурентоспособности предприятия на основе анализа процессов её информационных систем и их развитие [1, 11, 12, 17].

* ***Шепелёва Ольга Юрьевна,*** *ассистент кафедры информатики Санкт-Петербургского государственного экономического университета, г. Санкт-Петербург, Российская Федерация.*
E mail: shepeleva-olga@list.ru

Шепелёв Пётр Юрьевич, *магистрант Санкт-Петербургского государственного экономического университета, г. Санкт-Петербург, Российская Федерация.*
E mail: peter_sh@mail.ru

Газуль Станислав Михайлович, *кандидат экономических наук, старший преподаватель кафедры информатики Санкт-Петербургского государственного экономического университета, г. Санкт-Петербург, Российская Федерация.*
E mail: stanislav@gazul.ru

Анализ системы менеджмента предприятия

Интегральным показателем эффективности системы менеджмента информационной безопасности предприятия при этом может выступать оценка времени реакции системы на события:

$$T_{\text{рсИБ}} = \sum_{i=1}^{k} (T_{\text{обнИБ}i} + T_{\text{блокИБ}i} + T_{\text{регИБ}i} + T_{\text{оповИБ}i}),$$

где k — количество атрибутов, подлежащих измерению; $T_{рсИБ}$ — время реакции система менеджмента компании на событие; $T_{обнИБi}$ — время обнаружения события; $T_{блокИБi}$ — время блокирования несанкционированных действий при нарушении информационной безопасности; $T_{регИБi}$ — время регистрации события (ИБ); $T_{оповИБi}$ — время оповещения персонала службы информационной безопасности о выявленном событии.

Динамика $T_{рсИБ}$ позволяет оценить состояние системы в целом и результативность принимаемых мер и средств управления, так как своевременная реакция на событие становится возможной только при качественно налаженном взаимодействии IT-специалистов, риск-менеджеров и сотрудников службы безопасности с сотрудниками, обеспечивающими экономическую и кадровую безопасность, согласно предлагаемому процессу (рис. 1).

Хотя широкое использование информационных технологий и переход России к цифровой экономике [9, 10] позволяют говорить о серьезном увеличении объемов перерабатываемой информации [16], стоит заметить, что развиваются и формы несанкционированного доступа [6] к информационным ресурсам фирм, которые увеличивают риск потери капитала, репутации и всего бизнеса. Поэтому количественное измерение *эффективности* подсистемы информационной безопасности предприятия как элемента системы его стратегического управления является актуальной задачей для научного исследования.

Кроме этого, важно понимать, что из-за сложности и многомерности системы с огромным объемом данных, требующих постоянного обновления, менеджеры по ИБ часто перегружены и не могут самостоятельно разработать эффективные показатели оценки системы в целом, сосредотачиваясь в основном на реализации технических целей и контроле их достижения, в то время как лишь немногие компании разрабатывают комплексные многомерные оценки, и еще меньшее число систематически и непрерывно используют их в измерении собственных позиций информационной безопасности [14].

Здесь важно заметить, что ни одна система безопасности не способна дать 100%-ную гарантию защищенности [7] коммерческой информации. Но именно многоуровневая комплексная система защиты данных однозначно эффективнее в сравнении с применением отдельных методов обеспечения информационной безопасности, разделяемых на технические, административные, правовые, физические.

Стремительно растущий рынок информационной безопасности в России подтверждает ее востребованность в современных условиях (рис. 2), и ИБ должна быть включена в перечень целей стратегического управления каждым коммерческим предприятием вне зависимости от его размера, а не ограничиваться требованиями технического и организационного характера [15].

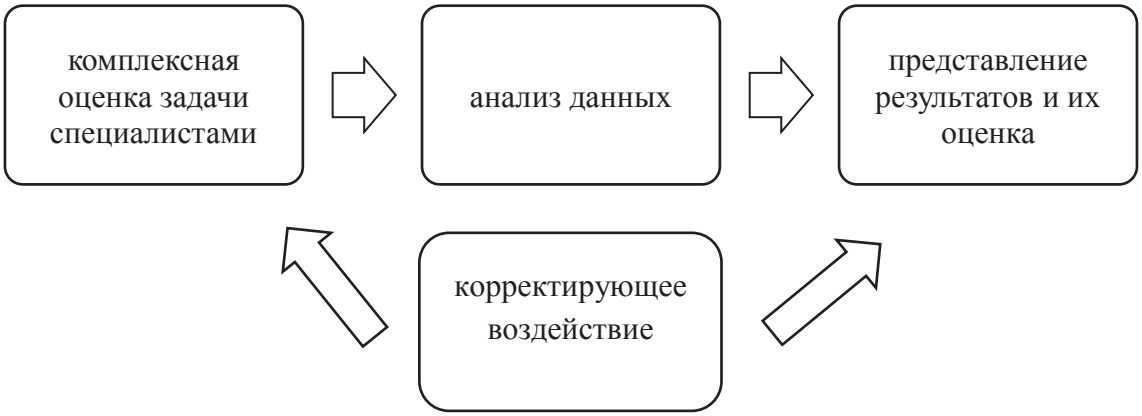

Рис.1. Процесс взаимодействия специалистов на основе непрерывного подхода «планирование-выполнение-проверка»

Около половины хакерских атак на коммерческие предприятия приходится на малый и средний бизнес. Безусловно, финансовые и репутационные потери крупных предприятий от разовых инцидентов могут выглядеть более впечатляюще, однако развиты в области обеспечения информационной безопасности они куда больше, чем малые и средние, реагирующие на необходимость расходов на комплексную оценку защищенности фирмы как на «ненужную» статью, препятствующую, с точки зрения лиц, принимающих решения, адекватному стратегическому развитию. То есть их менеджеры используют менее формализованные про-

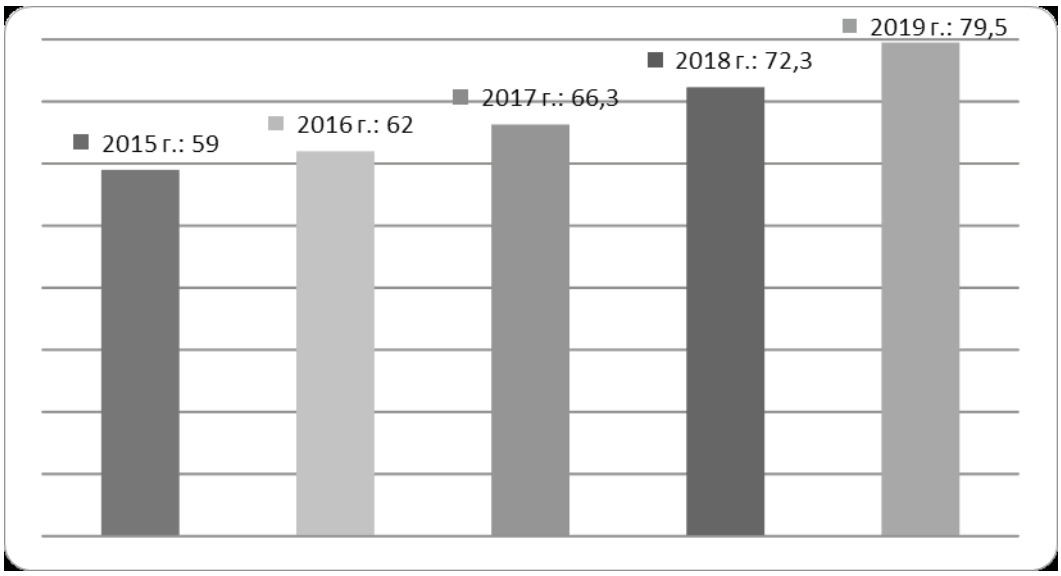

Рис. 2. Объем рынка информационной безопасности в России, млрд руб.

цедуры оценки, а значит, имеют и менее качественную информацию для прогнозирования инцидентов безопасности.

Соответственно, в России важно сосредоточиться на поддержке малого и среднего бизнеса, где ситуация с безопасностью в деловой среде является более критичной и может оказать существенное влияние на общую информационную и экономическую безопасность страны [13]. Здесь стоит обратить внимание еще на один фактор измерения и оценки системы информационной безопасности предприятия как составляющей части стратегического управления его развитием [5], а именно, на установление качественных подходов к измерению в ущерб разработке количественных методов.

Анализ литературы по теме исследования

Для достижения *цели исследования*, необходимо привести результаты литературного обзора. Анализ научных работ российских и зарубежных авторов показал, что в настоящее время разрабатываются *два базовых подхода* к оценке эффективности информационной безопасности:

– с точки зрения оценки рисков и уязвимостей;

– с точки зрения оценки метрик управления в соответствии со стандартами.

В первом случае возникают сложности с динамическим характером угроз [2—4], во втором — с большим количеством и разным характером требований к эффективному, гибкому и устойчивому состоянию системы [5].

Авторское исследование в большей степени базируется на втором подходе и представляет собой оценку возможностей стратегического управления информационной безопасностью предприятия в следующих аспектах: техническая безопасность, управление информационной системой, управление ресурсами, управление уязвимостями и риск-менеджмент, администрирование и управление безопасностью данных, управление непрерывностью бизнес-процессов, по которым экспертами предприятию выставляются оценки.

Предложенный вариант второго подхода требует проведения опроса, эксперимента и оценки уязвимости для анализа трех функциональных областей: люди, бизнес-процессы предприятия и используемые технологии.

Результаты литературного обзора показали, что методология, основанная на фактических данных, на основе всеобъемлющих рамок, позволит принимать более обоснованные и эффективные решения, а значит, существует потребность в разработке обобщенной *модели*, способной выделить наиболее значимые факторы успеха оценки эффективности информационной безопасности предприятия.

Модель

Для разработки инструмента, позволяющего оценить эффективность стратегического управления информационной безопасностью предприятия, использовалась международная стандартизованная среда *COBIT*, в которой показатель эффективности связан с количеством выявленных проблемных ситуаций и основными процессами *ITIL*/*ITSM* — оптимального сочетания людей, процессов и информационных технологий.

Полученные результаты продемонстрировали отрицательную зависимость между несоблюдением требований и наличием недостатков у системы внутреннего контроля с показателями информационной безопасности, тогда как предыдущий опыт организации при возникновении инцидентов с ИБ сказывался положительно.

Существующие модели оценки ИБ предприятия как составляющей части его стратегического корпоративного управления в основном сосредоточены либо на

производительности в конкретных областях, таких как стратегия ИБ, политика ИБ, комплаенс сотрудников, управление уязвимостями, программное обеспечение и др., либо на производительности конкретных секторов экономики. Это влечет за собой проблемы, связанные с отсутствием единой политики информационной безопасности, ограниченным использованием управления рисками и несвоевременным принятием решений в отношении управления уязвимостями и инцидентами ИБ.

Изучение существующих количественных моделей показало, что они основаны преимущественно на оценке управления информационной безопасностью предприятия путем использования опросов и показателей самооценки соответствия отраслевым метрикам, которые не дают общую применимую на практике картину или узко направлены на оценку рисков, результаты которой трудно применимы для стратегического управления развитием предприятия в реальных условиях.

В авторской модели для обеспечения постоянного улучшения результатов измерений используются ключевые показатели эффективности (*KPI*), которые были установлены на основе нормативных требований и международных стандартов информационной безопасности (*ISO/IEC 27k*, *COBIT* и др.).

Кроме этого, модель обеспечивает представление результатов для облегчения процесса принятия решений, поскольку менеджер получает информацию о конкретных проблемах и общей позиции безопасности в организации, а следовательно, может ставить достижимые цели и выбирать наилучшие альтернативы, своевременно корректируя меры воздействия и оптимально перераспределяя доступные ресурсы.

Модель рассматривает наиболее значимые факторы, влияющие на достоверность оценки информационной безопасности предприятия как составляющей части стратегического корпоративного управления (см. табл. 1).

Таблица 1

Значимые факторы успеха оценки эффективности ИБ предприятия

№ п/п	Название фактора	Описание фактора
1	Физический контроль информационной безопасности	Включает обеспечение мер физической безопасности внутри и за пределами организации посредством ограничения доступа к зданиям и оборудованию, контроля сохранности источников информации, контроля безопасности в прилегающих к объектам защиты районах.
2	Технический контроль информационной безопасности	Заключается в контроле работы информационных систем, выявлении аномалий и предотвращении несанкционированных действий посредством наложения технических ограничений на пользовательские возможности в пределах использования данных, технических средств, приложений и сетей.
3	Управление информационными ресурсами	Состоит в поддержании конфиденциальности и целостности информационных ресурсов на всех стадиях жизненного цикла информации. Включает шифрование, создание резервных копий, безопасное уничтожение данных, организацию защищенного удаленного доступа и др. аспекты.
4	Управление HR (Human resources)	Состоит в проверке компетенций и мотивов всех пользователей, взаимодействующих с информацией временно или на постоянной основе, проведении мероприятий повышения уровня осведомлённости о важности информационной безопасности.
5	Управление информационными рисками и обработка происшествий	Заключается в выявлении, анализе и минимизации рисков информационного характера при соблюдении рационального соотношения между рисками и инвестиционной привлекательностью. Подразумевает реагирование на происшествия и ликвидацию угроз при появлении.
6	Поддержка со стороны руководства	Наибольшая ответственность в вопросах информационной безопасности на предприятии возлагается на руководство, что обязывает его создать качественно организованные условия в текущей и стратегической перспективах. Подразумевается создание механизмов обратной связи между пользователями с целью формирования потребностей.
7	Политика ИБ и комплаенс	Состоит в неразрывности связей между стратегией и политикой управления информационной безопасностью, описании запрещенных действий, учете пользовательских нужд и соблюдении актуальных нормативных актов.
8	Степень зрелости управления безопасностью	Подразумевает необходимость в высокой оценке уровня зрелости управления безопасностью для обеспечения информационной безопасности, что может быть достигнуто за счет функционирования ИБ в форме отдельного бизнес-процесса, и поддержании позитивных настроений среди сотрудников предприятия в отношении политики ИБ.
9	Отношения с третьими лицами	Включает анализ уязвимостей в рамках отношений с партнерами и клиентами, исследования степени развитости в вопросе информационной безопасности. Подразумевает кооперацию между организациями для создания общего информационно-защищенного пространства.
10	Связь с внешней средой	Состоит в необходимости учитывать такие глобальные сферы, как социальная, экономическая и политическая при формировании гибкой системы информационной безопасности.

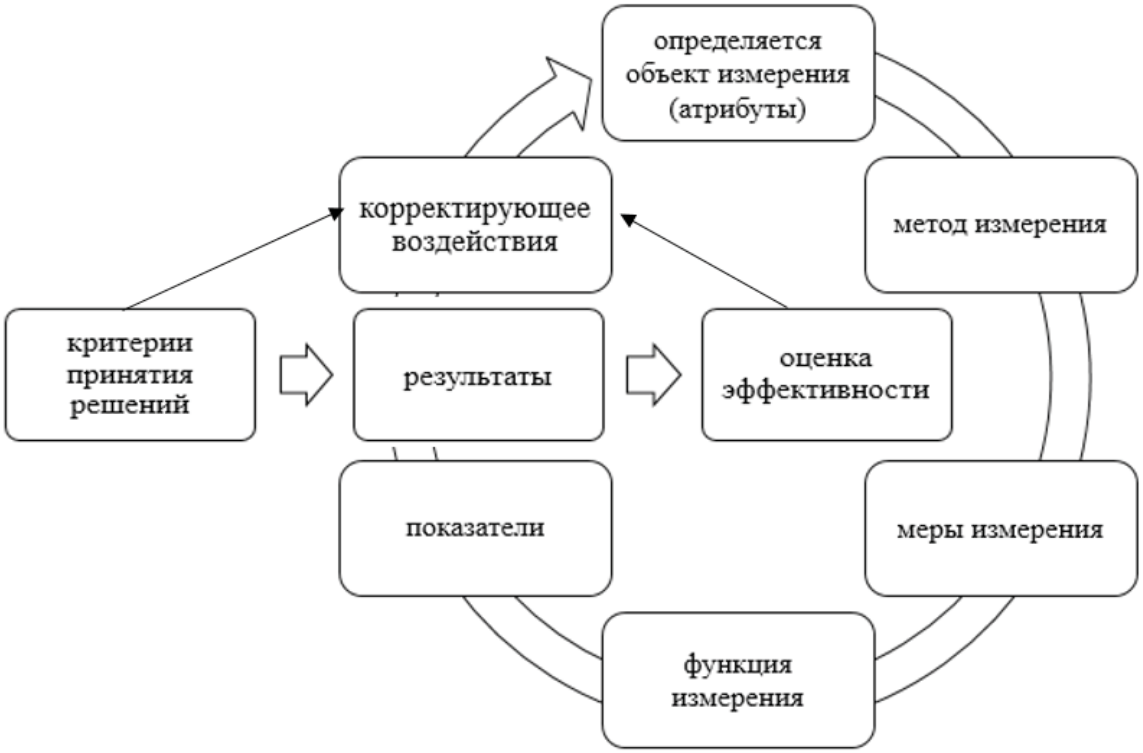

Рис. 3. Модель измерений, проводимых в структуре системы менеджмента информационной безопасности предприятия

Количество включаемых в модель элементов (см. таблицу) может быть увеличено в зависимости от предметной области применения модели, рыночной конъюнктуры и других внешних факторов, однако результаты авторского анализа практической литературы по данному направлению показывают, что выбранные в таблице факторы являются наиболее значимыми для учёта.

Её использование позволяет оценить уровень ИБ предприятия с трех сторон: технической, организационной и социальной. В соответствии с данными факторами специалисты оценивают текущий уровень информационной безопасности на предприятии и представляют результаты работы руководству, после чего анализируется разрыв актуальных и требуемых уровней факторов и принимается решение о реализации действий по устранению разрывов и внесению изменений в систему оцениваемых показателей.

На базе разработанной модели создается система измерений, для которых разрабатываются и вводятся конструктивные значения, исходя из потребностей достижения значимого фактора ИБ предприятия (рис. 3).

Они позволяют исследовать взаимное влияние показателей качества объектов измерений при сборе данных датчиками на информационную потребность, получать воспроизводимые, объективные и пригодные результаты для своевременного принятия управленческого решения.

Заключение

Таким образом, рассмотрен процесс многофакторного анализа [8] информационной безопасности для предприятий малого и среднего бизнеса путем представления модели, позволяющей оценить технические, организационные и социальные аспекты.

Представляется целесообразным прийти к пониманию, что существенное негативное воздействие на ИБ оказывают информационные риски и некомпетентность в управлении ими. Использование представленной авторами модели позволит не просто выяснить текущий уровень информационной безопасности на российских малых и средних предприятиях, а будет способствовать устранению уязвимостей в корпоративных информационных системах посредством реализации таких действий, как:

– отслеживание современных тенденций и трендов на рынке ИБ;

– создание и поддержание функционирующей системы управления безопасностью;

– управление качеством;

– четкое распределение ответственности между ролями, задействованными в обеспечении информационной безопасности;

– тотальное осведомление пользователей о важности ИБ;

– внедрение ИБ в перечень стратегических целей;

– непрерывное наблюдение за процессами и результатами деятельности;

– создание и поддержка системы для коммуникаций между пользователями.

Для этого предлагается:

– учитывать в стратегии развития предприятия потребность в обеспечении независимости управления его информационной безопасностью наряду с потребностью непрерывного управления качеством;

– четко регламентировать ответственных за информационную безопасность и культуру, их контроль и развитие;

– наряду с целью обеспечения эффективности бизнес-процессов, ставить цель обеспечения информационной безопасности предприятия, осуществлять её непрерывный мониторинг и контроль, обеспечивать координацию между сотрудниками, понимание целей и задач, взаимозависимости стратегии безопасности и целей организации.

Литература

1. Вертакова Ю. В., Плотников В. А. Развитие тенденций мирового кризиса под влиянием пандемии COVID-19 // Экономика коронакризиса: вызовы и решения: Сб. науч. тр. (27 апреля 2020 г.) / ИПУ РАН / Под ред. Р. М. Нижегородцева. М. : НИПКЦ-Восход-А, 2020. С. 32—35.
2. Зобнин А. Д., Кияев В. И. Биометрические технологии как механизм обеспечения информационной безопасности в цифровой экономике // Hypothesis. 2020. № 2 (11). С. 11—16.
3. Карцхия А. А., Макаренко Г. И., Сергин М. Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18—23.
4. Кияев В. И., Дятлов К. А. Использование IOT-технологий для мониторинговых систем в хозяйственной деятельности // Hypothesis. 2020. № 2 (11). С. 17—25.
5. Кияев В. И. Мультиагентные технологии в системах мониторинга и управления // Актуальные вопросы развития современной науки: теория и практика: Тр. XLI науч. конференции (1 марта — 30 апреля 2019 г.) / СПбГЭУ. СПб. : СПбГЭУ, 2019. С. 17—20.
6. Ловцов Д. А. Информационная безопасность эргасистем: нетрадиционные угрозы, методы, модели // Информация и космос. 2009. № 4. С. 100—105.
7. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/1994-1404-2017-3-66-74.
8. Минаков В. Ф., Шепелёва О. Ю., Лобанов О. С. Многофакторная модель обеспечения безопасности конфиденциальных данных / Правовая информатика. 2020. № 1. С. 40—46. DOI: 10.21681/1994-1404-2020-1-40-46.
9. Минаков В. Ф., Минакова Т. Е., Шепелёва О. Ю. Модель конвергенции в цифровой экономике // Информатика: проблемы, методы, технологии: Тр. XX Междунар. науч.-метод. конф. (13—14 февраля 2020 г.) / ВорГУ. Воронеж : Вэлборн, 2020. С. 1504—1509.
10. Минаков В. Ф. Конвергенция и дивергенция в экономике: волновая природа // Информационные приоритеты и экономические ориентиры социального развития регионов России: Тр. Всеросс. науч.-практ. конф. (28—29 мая 2020 г.) / СтГАУ. Ставрополь : Агрус, 2020. С. 303—309.
11. Плотников В. А. Перспективы трансформации социально-экономической системы под воздействием цифровизации // Современное состояние экономических систем: экономика и управление: Тр. II Междунар. науч. конф. (23—24 марта 2020 г.) / ТГУ. Тверь : СФК-офис, 2020. С. 6—11.
12. Плотников В. А. Экономические системы как объект изучения в цифровую эпоху // Социально-экономическое развитие в условиях цифрового общества: Тр. IX Национ. науч.-прак. конф. Института магистратуры с международным участием (20—21 апреля 2020 г.) / СПбГЭУ. СПб. : СПбГЭУ, 2020. С. 113—118.
13. Трофимов В. В., Трофимова Л. А. Информационная безопасность в концепции национальной системы управления данными // Национальная безопасность России: актуальные аспекты: Тр. Всеросс. науч.-прак. конф. (30 июля 2019 г.) / ГНИИ «Нацразвитие». СПб. : ГНИИ «Нацразвитие», 2019. С. 14—19.
14. Barabanov A.V., Markov A.S., Tsirlov V.L. Tendencies in international evaluation of it-products for compliance with information safety requirements // Information Technologies for Intelligent Decision Making Support. Proceedings of the 5th All-Russian Conference (15-16 May 2017) / УГАТУ. Уфа : УГАТУ, 2017. С. 111—114.
15. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological issues related to the evaluation of the communication networks equipment conformity to the information security requirements // Information Technologies for Intelligent Decision Making Support. Proceedings of the 5th All-Russian Conference (15-16 May 2017) / УГАТУ. Уфа : УГАТУ, 2017. С. 105—110.
16. Vertakova Y., Plotnikov V., Babich T. Conceptual framework of state economic policy in the technological and social transformation conditions // E3S Web of Conferences. Topical Problems of Green Architecture, Civil and Environmental Engineering, TPACEE 2019. 2020. С. 11016.

17. Pirogova O., Plotnikov V. Management of enterprise development based on adaptive value model in digital conditions // E3S Web of Conferences. Topical Problems of Green Architecture, Civil and Environmental Engineering, TPACEE 2019. 2020. C. 10024.

Рецензент: ***Марков Алексей Сергеевич,*** *доктор технических наук, старший научный сотрудник, профессор МГТУ им. Н.Э.Баумана, г. Москва, Россия.*
E-mail: a.markov@bmstu.ru

ENTERPRISE INFORMATION SECURITY ASSESSMENT AS A PART OF STRATEGIC CORPORATE GOVERNANCE

Ol'ga Shepeleva, *Assistant Professor at the Department of Informatics of the Saint Petersburg State University of Economics, Saint Petersburg, Russian Federation.*
E-mail: *shepeleva-olga@list.ru*

Petr Shepelev, *master's student at the Saint Petersburg State University of Economics, Saint Petersburg, Russian Federation.*
E-mail: *peter_sh@mail.ru*

Stanislav Gazul', *Ph.D. (Economics), Senior Lecturer at the Department of Informatics of the Saint Petersburg State University of Economics, Saint Petersburg, Russian Federation.*
E-mail: *stanislav@gazul.ru*

Keywords: *information security, economic efficiency, risk management, strategic corporate governance, information systems, model, factors, assessments.*

Abstract.

Purpose of the work: *studying modern approaches to assessing the efficiency of information security of small and medium-sized businesses in Russia and improving the methodological basis of the theory of assessing the efficiency of enterprise information security strategic management system with a view to increasing the stability of its functioning and raising its competitiveness based on the use of innovative methods.*

Methods used: *it is proposed to use general scientific methods, including mathematical modelling ones which allow, based on the results of a statistical analysis of a sample of businesses taken from the Federal Government Statistics Service database, to develop a model using the most significant factors impacting the reliability of assessment of enterprise information security as a component of strategic corporate governance.*

Results obtained: *in the paper, assessing the efficiency of information security is considered fundamental for the system of information management of the strategic development of a modern enterprise. Based on the multidimensional social-cum-technical approach, an assessment of efficiency of the information security management system of Russian enterprises was carried out. The results show an underdevelopment of measures related to the optimisation of using information resources and risk management specifically at the strategic management level, while enterprises have considerable opportunities for quantitatively measuring information security indicators. Therefore the authors developed a model which considers the most significant factors impacting the reliability of assessment of information security of a small and medium-sized business in Russia as a component of strategic corporate governance and can be modified depending on its profile.*

References

1. Vertakova Iu. V., Plotnikov V. A. Razvitie tendentsii mirovogo krizisa pod vliianiem pandemii COVID-19. Ekonomika koronakrizisa: vyzovy i resheniia: Sb. nauch. tr. (27 aprelia 2020 g.). IPU RAN. Pod red. R. M. Nizhegorodtseva. M. : NIPKTs-Voskhod-A, 2020, pp. 32-35.
2. Zobnin A. D., Kiiaev V. I. Biometricheskie tekhnologii kak mekhanizm obespecheniia informatsionnoi bezopasnosti v tsifrovoi ekonomike. Hypothesis, 2020, No. 2 (11), pp. 11-16.
3. Kartskhiia A. A., Makarenko G. I., Sergin M. Iu. Sovremennye trendy kiberugroz i transformatsiia poniatiia kiberbezopasnosti v usloviiakh tsifrovizatsii sistemy prava. Voprosy kiberbezopasnosti, 2019, No. 3 (31), pp. 18-23.
4. Kiiaev V. I., Diatlov K. A. Ispol'zovanie IOT-tekhnologii dlia monitoringovykh sistem v khoziaistvennoi deiatel'nosti. Hypothesis, 2020, No. 2 (11), pp. 17-25.

5. Kiiaev V. I. Mul'tiagentnye tekhnologii v sistemakh monitoringa i upravleniia. Aktual'nye voprosy razvitiia sovremennoi nauki: teoriia i praktika: Tr. XLI nauch. konferentsii (1 marta -– 30 aprelia 2019 g.). SPbGEU. SPb. : SPbGEU, 2019, pp. 17-20.
6. Lovtsov D. A. Informatsionnaia bezopasnost' ergasistem: netraditsionnye ugrozy, metody, modeli. Informatsiia i kosmos, 2009, No. 4, pp. 100-105.
7. Lovtsov D. A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74. DOI: 10.21681/1994-1404-2017-3-66-74.
8. Minakov V. F., Shepeleva O. Iu., Lobanov O. S. Mnogofaktornaia model' obespecheniia bezopasnosti konfidentsial'nykh dannykh. Pravovaia informatika, 2020, No. 1, pp. 40-46. DOI: 10.21681/1994-1404-2020-1-40-46.
9. Minakov V. F., Minakova T. E., Shepeleva O. Iu. Model' konvergentsii v tsifrovoi ekonomike. Informatika: problemy, metody, tekhnologii: Tr. XX Mezhdunar. nauch.-metod. konf. (13-14 fevralia 2020 g.). VorGU. Voronezh : Velborn, 2020, pp. 1504-1509.
10. Minakov V. F. Konvergentsiia i divergentsiia v ekonomike: volnovaia priroda. Informatsionnye prioritety i ekonomicheskie orientiry sotsial'nogo razvitiia regionov Rossii: Tr. Vseross. nauch.-prakt. konf. (28-29 maia 2020 g.). StGAU. Stavropol' : Agrus, 2020, pp. 303-309.
11. Plotnikov V. A. Perspektivy transformatsii sotsial'no-ekonomicheskoi sistemy pod vozdeistviem tsifrovizatsii. Sovremennoe sostoianie ekonomicheskikh sistem: ekonomika i upravlenie: Tr. II Mezhdunar. nauch. konf. (23-24 marta 2020 g.). TGU. Tver' : SFK-ofis, 2020, pp. 6-11.
12. Plotnikov V. A. Ekonomicheskie sistemy kak ob"ekt izucheniia v tsifrovuiu epokhu. Sotsial'no-ekonomicheskoe razvitie v usloviiakh tsifrovogo obshchestva: Tr. IX Natsion. nauch.-prak. konf. Instituta magistratury s mezhdunarodnym uchastiem (20-21 aprelia 2020 g.). SPbGEU. SPb. : SPbGEU, 2020, pp. 113-118.
13. Trofimov V. V., Trofimova L. A. Informatsionnaia bezopasnost' v kontseptsii natsional'noi sistemy upravleniia dannymi. Natsional'naia bezopasnost' Rossii: aktual'nye aspekty: Tr. Vseross. nauch.-prak. konf. (30 iiulia 2019 g.). GNII "Natsrazvitie". SPb. : GNII "Natsrazvitie", 2019, pp. 14-19.
14. Barabanov A.V., Markov A.S., Tsirlov V.L. Tendencies in international evaluation of it-products for compliance with information safety requirements. Information Technologies for Intelligent Decision Making Support. Proceedings of the 5th All-Russian Conference (15-16 May 2017). UGATU. Ufa : UGATU, 2017, pp. 111-114.
15. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological issues related to the evaluation of the communication networks equipment conformity to the information security requirements. Information Technologies for Intelligent Decision Making Support. Proceedings of the 5th All-Russian Conference (15-16 May 2017). UGATU. Ufa : UGATU, 2017, pp. 105-110.
16. Vertakova Y., Plotnikov V., Babich T. Conceptual framework of state economic policy in the technological and social transformation conditions. E3S Web of Conferences. Topical Problems of Green Architecture, Civil and Environmental Engineering, TPACEE 2019. 2020. P. 11016.
17. Pirogova O., Plotnikov V. Management of enterprise development based on adaptive value model in digital conditions. E3S Web of Conferences. Topical Problems of Green Architecture, Civil and Environmental Engineering, TPACEE 2019. 2020. P. 10024.