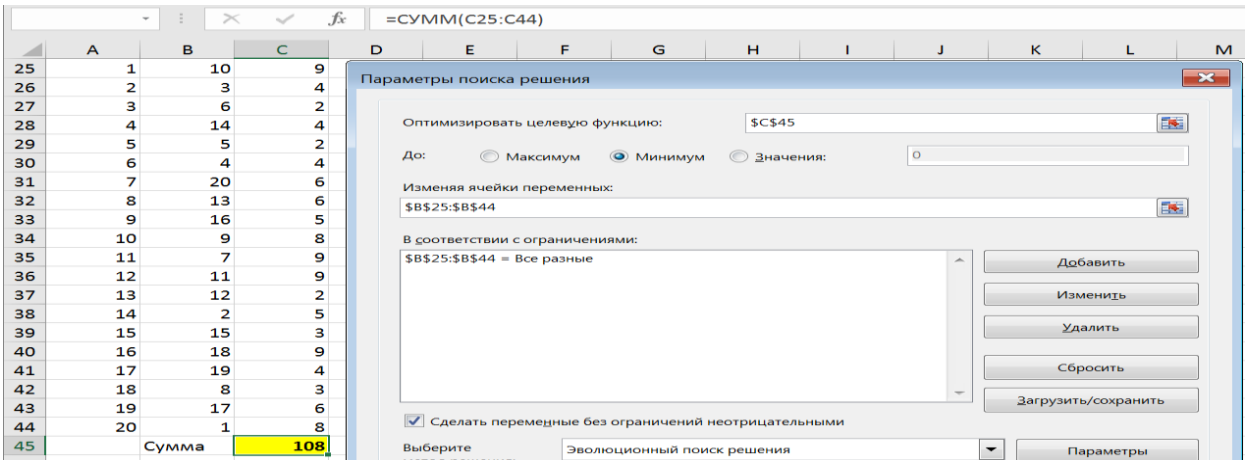

Рисунок 8 – Фрагмент окончания решения задачи планирования маршрута в среде *Excel*

Заключение. В статье рассмотрена методика планирования указанных видов транспортных перевозок, которая обеспечивает эффективное и негромоздкое решение соответствующих конкретных задач в стандартных компьютерных средах *MatLab*и *Excel.*

ЛИТЕРАТУРА

1. Титова, Е. И. Разрешимость транспортной задачи по критерию времени / Е. И. Титова, А. В. Чапрасова // Молодой ученый. – 2014. – №4. – С. 36-38. – URL https://moluch.ru/archive/63/9712/ (дата обращения: 02.02.2020).
2. Костевич, Л.С. Математическое программирование: Информ. технологии оптимальных решений / Л.С. Костевич. – Минск: Новое знание, 2003. – 424 с.
3. Оптимизация работы автотранспортных предприятий: методические указания для выполнения дипломных работ по специальности 1-25 01 07 «Экономика и управление на предприятии» / БГАТУ, кафедра моделирования и прогнозирования экономики АПК; сост. Б.М.Астрахан. – Минск. 2005.– 30 с.
4. Применение информационных технологий для оптимизации поставок сжиженного газа сельским потребителям / Б.М. Астрахан [и др.] // Агропанорама. – 2009. – № 1. – С. 34-39.
5. Винстон, У. Бизнес-моделирование и анализ данных. Решение актуальных задач с помощью MicrosoftExcel. 5-е издание / У. Винстон. – СПб.: Питер, 2018. – 864 с.
6. Астрахан, Б.М. Информационные технологии в логистике ОАО «1-ая Минская птицефабрика» / Б.М. Астрахан, П.В. Клавсуть//Современные проблемы освоения новой техники, технологий, организации технического сервиса в АПК. Материалы Междунар. науч.-практ. конф. «Белагро-2019» (Минск, 6-7 июня 2019 г.). – Минск: БГАТУ. – 2019. – С. 404-408.

УДК 334.7

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИНИМАТЕЛЬСТВА В УСЛОВИЯХ РИСКОВ И УГРОЗ ЦИФРОВОЙ ЭКОНОМИКИ

канд. экон. наук, доцент С.Н. ***Барейко,*** *Ленинградский государственный университет им. А.С. Пушкина*

Резюме - в настоящее время в мире происходят глобальные перемены, которые связаны с появлением новых цифровых технологий, бурным развитием цифровых коммуникаций и внедрением инновационных технологий в экономику. Современные исследования показывают, что осуществляемый в России процесс последовательных социально-экономических преобразований делает особо актуальным интерес к институту предпринимательства как к одному из главных условий эффективного функционирования рыночного механизма. В этой связипредпринимательским структурам необходимо в ускоренном режиме внедрять и использовать цифровые технологии в своих компаниях в целях обеспечения устойчивого роста и обеспечения конкурентоспособности [1].

*Ключевые слова**: предпринимательство, экономическая и информационная безопасность, риски, угрозы, цифровая экономика, информационная инфраструктура.*

Введение.Устойчивое развитие экономики России неразрывно связано с цифровой экономикой. Основная задача «Программы развития цифровой экономики в Российской Федерации до 2035 года» – заключается в формировании системы мер поддержки и стимулирования, которая обеспечивает мотивацию субъектов финансово- хозяйственной деятельности к цифровым инновациям и исследованиям в области цифровых технологий. Эффективное развитие предпринимательства, в частности перевод его на инновационный путь развития, становится важнейшей задачей, требующей проведения всесторонних научных исследований [8]. Разработка национальных программ развития экономики нового поколения, включающая вопросы развития и внедрения инновационных технологий, становится задачей стратегической важности в целях обеспечения

национальной безопасности России. Модернизация традиционных производственных отраслей и отраслей услуг на основе их цифровизации является мировым трендом. Для реализации целей принципиальное значение имеет адекватная цифровизация государственного управления.

Основная часть. Основные мероприятия по цифровой трансформации государственного управления сформулированы в рамках разработанного федерального проекта «Цифровое государственное управление», включенного в состав национального проекта «Цифровая экономика Российской Федерации» [1]. По данным российского Национального координационного центра по компьютерным инцидентам в 2018 году было совершено более 4,3 млрд цифровых воздействий на критическую информационную инфраструктуру России. Чаще всего с атаками сталкиваются банки и органы власти в России. При этом спецслужбы отмечают увеличения числа попыток хакерских атак на информационную инфраструктуру критически важных объектов России, в том числе, в энергетике и на транспорте [5,9]. Противодействие экономическим правонарушениям и преступлениям на любом предприятии предполагает создание многоцелевой системы управления, учёт норм международных стандартов, применение более совершенных технологий в принятии управленческих решений, обоснование новых направлений кадровой политики, многопрофильную подготовку кадров.

В этой связи, в целях создания условий для повышения благосостояния и качества жизни граждан России, разработана Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы, утвержденная Указом Президента Российской Федерации от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы". Правовой основой Программы развития цифровой экономики в Российской Федерации является Конституция Российской Федерации, Федеральный закон от 28 июня 2014 года № 172-ФЗ «О стратегическом планировании в Российской Федерации»[8].

Национальная безопасность государства — это состояние информационной и экономической сферы государства, в рамках которой обеспечивается безопасность страны и удовлетворяются интересы отдельных граждан, объединений и общества в целом [2]. Поэтому противодействие экономическим правонарушениям и преступлениям на любом предприятии предполагает создание многоцелевой системы управления, учёт норм международных стандартов, применение более совершенных технологий в принятии управленческих решений, обоснование новых направлений кадровой политики, многопрофильную подготовку кадров. И это связано не только с общим кризисным состоянием российской экономики, сохраняющейся инфляцией, низким курсом рубля и прочими макроэкономическими деформациями, но и с рядом специфических факторов, усиливающих активизацию угроз экономической безопасности хозяйствующих субъектов [4]. К угрозам, характеризующим экономическую сферу, можно отнести непрофессионализм в области ведения финансово-хозяйственной деятельности, хищения, взяточничество, кражи, контрабанду и т.д.

К социальным угрозам относятся: безработица, нищета, социальное неравенство и т.д.

К информационным угрозам можно отнести: нарушение конфиденциальности, разглашение информации, несоблюдение коммерческой тайны, промышленный шпионаж, конкурентную разведку и т.д. При этом угрозы представляются в следующем соотношении: 82% угроз, связанные с действиями сотрудников организаций, либо при их прямом или опосредованном участии; 17% - внешние угрозы; 1% представляют собой угрозы со стороны случайных лиц.

Распространенность и развивающиеся тенденции в использовании информационных технологий приводят к бурному росту числа угроз и рисков в секторе информационной безопасности. Возможность обработки большей части данных в электронном виде способствовала расширению перечня угроз, которые связаны с разглашением, хищением и порчей информации, что может принести крупные материальные и репутационные риски для хозяйствующего субъекта. Для информации являющейся собственностью предприятия выделяют следующие виды угроз (табл. 1).

Таблица 1- Угрозы внутренней информации хозяйствующего субъекта

Виды угроз	Характерные черты
Характер угроз, связанных с конфиденциальностью информации и программного обеспечения	Нелегальный доступ к данным. Утечка информации
Риски повреждения файлов и информации	Атаки хакеров, которые в конечном итоге, могут повлечь за собой искажение и потерю информации
Риски и угрозы доступности информации	Недоступность использования информации законным пользователем
Отказ от исполнения транзакций	В целях избегания ответственности отказ пользователя от передаваемой им же информации

Источник: разработано автором.

Информационная структура предприятий состоит из набора сложных систем, включающих в себя большой объём стратегических ресурсов. При отсутствии необходимого контроля, конкуренты могут нанести ущерб компании, причиняя вред деловой репутации организации, узнавать и разглашать конфиденциальную информацию, создавать необходимость восстановления нарушенных ресурсов и дезорганизировагь работу всего предприятия. Сложность взаимоотношений субъектов информационной сферы предопределяет

множественность информационных опасностей, которые связаны с уровнем достоверности и надежности, как получаемой информации, так и генерируемой или преобразуемой. Все множество опасностей можно разделить на две группы:

- контроль информации или ее несанкционированное получение;
- разрушение, уничтожение, изменение информации.

В связи со ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации» субъектам информационной сферы необходимо предпринять меры информационной безопасности по трем направлениям (рис 1):

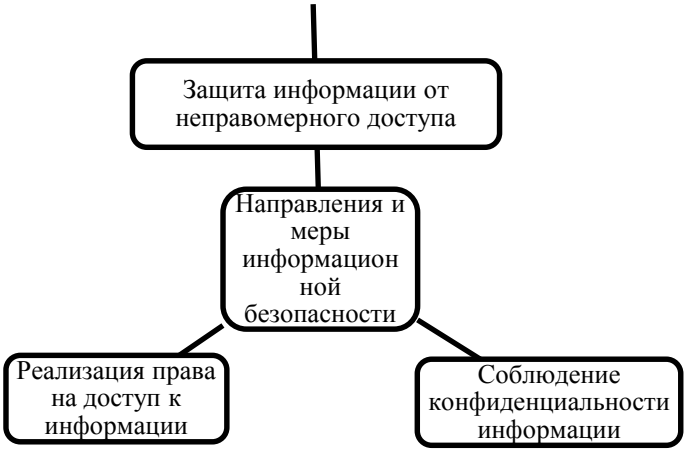

Рисунок 1- Направления и меры информационной безопасности
Источник: разработано автором.

Среди множества проблем социально-экономического развития России в условиях формирования глобального постиндустриального общества заметное место занимает организация устойчивого функционирования и безопасности использования информационных систем и информационно-коммуникационных сетей, обеспечивающих экономическую деятельность. По мере усложнения информационной инфраструктуры бизнеса влияние данного фактора на результаты деятельности коммерческих организаций будет возрастать. Это наглядно видно на примере развития экономики США, для которых обеспечение компьютерной безопасности стало одним из национальных приоритетов XXI в. Проблема обеспечения информационной безопасности бизнеса имеет много аспектов, но все они так или иначе объединены необходимостью стандартизации принимаемых решений – своеобразной платой за преодоление «проклятия размерности», порождаемого сложностью управляемых процессов.

Анализ международного обеспечения информационной безопасности показывает, что разработка этой проблемы в мировом сообществе идет в основном по следующим направлениям (рис 2.)

Рисунок 2- Направления обеспечения экономической и информационной безопасности в мировом сообществе
Источник: разработано автором.

Одним из важных направлений обеспечения информационной безопасности в мире является защита электронных документов и электронной торговли. К основным задачам в этой области относятся: расширение правового поля; равноправное использование электронных форм информации наряду с другими видами

носителей; сокращение числа ограничений и барьеров в отношении создания, распространения и использования информационных продуктов и технологий. В настоящее время во многих странах ведется работа по принятию законов об электронной торговле и электронных документах. И речь идет не только о таких информационных гигантах, как США, аналогичные законы приняты в Республике Беларусь и даже Туркменистане [3]. Законодательством США в области информатизации и защиты информации предусмотрен ряд моментов: определение и закрепление государственной политики в области информатизации; обеспечение развитого производства и технологий; защита и организация информационных систем; защита прав граждан на информацию; регулирование прав разработчиков информационных программ.

Ответственность за злоупотребления при работе с информацией, предусмотренная в законодательствах различных развитых стран, характеризуется общими для всех этих стран правилами: установлена ответственность за нарушение порядка обработки и использования персональных данных; информационные (компьютерные) преступления расцениваются как преступления, которые представляют особую опасность для граждан, общества, государства и влекут за собой значительно более жесткие меры наказания, нежели аналогичные преступления, совершенные без применения компьютерной техники; попытка проникновения в систему, внедрение компьютерных вирусов и так далее рассматриваются как преступления. Целью национальной программы развития цифровой экономики является создание в России благоприятных организационных и нормативно-правовых условий для эффективного развития институтов цифровой экономики при участии государства, национального бизнес-сообщества и гражданского общества в целом [3].

Заключение. Бурное развитие информационных технологий и цифровой экономики в России, требуетновых подходов в целях обеспечения экономической и информационной безопасности современного предпринимательства.Среди множества проблем социально-экономического развития России в условиях формирования глобального постиндустриального общества заметное место занимает организация устойчивого функционирования и безопасности использования информационных систем и информационно-коммуникационных сетей, обеспечивающих экономическую деятельность. По мере усложнения информационной инфраструктуры бизнеса влияние данного фактора на результаты деятельности коммерческих организаций будет возрастать.

ЛИТЕРАТУРА

1.Абрамешина С.А. Развитие предпринимательства в условиях цифровой трансформации экономики // Научное сообщество студентов XXI столетия. Экономические науки: сб. ст. по мат. LXXIV междунар. студ. науч.-практ. конф. № 2(74).

2.Барейко С.Н. Развитие малого и среднего предпринимательства в России как один из ключевых факторов экономической и социальной стабильности//Национальная безопасность/notabene.-2019.-№1.С.49-55.

3.Барейко С.Н., Кожухина К.А. Экономическая и информационная безопасность России в условиях цифровой экономики//Наука Красноярья.2019. Т.8. №5. С.7-18.

4.Галочкина О.А., Костин К.Б., Кожухина К.А. Современное предпринимательство: содержание, особенности, риски: Монография / О.А. Галочкина, К.Б. Костин, К.А. Кожухина. — СПб: Университет при МПА ЕврАзЭС, 2019, стр. 256

5.Индикаторы цифровой экономики //Статистический сборник: Электронный ресурс]:[сайт] URL// https://www.hse.ru(дата обращения 20.11.2019).

6.Плотникова М.В. Направления повышения качества кредитных услуг на основе цифровых технологий [Текст] / М.В. Плотникова // Экономическая безопасность и качество. – № 1(30). – 2018. – Саратов: Саратовский социально-экономический институт (филиал) РЭУ им. Г.В. Плеханова, 2018. – С. 49-53.

7.Экономическая безопасность России. Общий курс [Электронный ресурс]: учебник / под ред. В.К. Сенчагова. – 5-е изд. (эл.). – Электрон. текстовые дан. (1 файл pdf. 818 с.). – М.: БИНОМ. Лаборатория знаний, 2015. – Режим доступа: http://www.bibliorossica.com/book.html?currBookId=21826 (дата обращения: 06.11.2019).

8.Развитие цифровой экономики в России. Программа до 2035 года [Электронный ресурс] // INNCLUB.info: информационно-аналитический портал клуба субъектов инновационного и технологического развития России: сайт. – Режим доступа: http://innclub.info/wp-content/uploads/2017/05/strategy.pdf (дата обращения: 06.12.2018).

9.Сайт НИСИПП: [Электронный ресурс]: [сайт] URL// http: www.nisse.ru(дата обращения 21.11.2019).

10.Сайт Росстата: [Электронный ресурс]: [сайт] URL//http://www.gks.ru(дата обращения 20.11.2019).

УДК 657

НЕОБХОДИМОСТЬ ОТРАЖЕНИЯ В ОТЧЕТНОСТИ ЧЕЛОВЕЧЕСКОГО КАПИТАЛА

*канд. экон. наук **Д.Ю. Бусыгин**, Минский филиал РЭУ им. Г.В. Плеханова, г.Минск*

Резюме – в статье рассматривается необходимость отражения в интегрированной отчетности данных о человеческом капитале компании.

Ключевые слова: человеческий капитал, интегрированная отчетность, стандарт.

Введение. В современных условиях развития экономики предоставление публичной нефинансовой отчетности компаниями становится неотъемлемым атрибутом ведения бизнеса. Решение вопросов, связанных с «зеленой экономикой», энергетической эффективностью, изменением климата, социальных последствий