УДК 330.341.2
DOI: 10.21209/2227-9245-2019-25-9-105-113

# ИНФОРМАЦИОННЫЕ УГРОЗЫ В УСЛОВИЯХ ЦИФРОВОЙ СЕТЕЗАЦИИ: МЕТОДИЧЕСКИЙ ИНСТРУМЕНТАРИЙ ОЦЕНКИ И МЕХАНИЗМ УПРАВЛЕНИЯ

# INFORMATION THREATS IN DIGITAL NETWORKS: METHODOLOGICAL TOOLS, ASSESSMENTS AND MANAGEMENT MECHANISM

**В. В. Акбердина,**
Институт экономики Уральского отделения РАН, г. Екатеринбург
akb_vic@mail.ru

**V. Akberdina,**
Institute of Economics, Ural Branch of the Russian Academy of Sciences, Yekaterinburg

**А. Д. Невская,**
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург
tikhonova.nastiya@mail.ru

**A. Nevskaya,** Ural Federal University named after the first President of Russia B. N. Yeltsin, Yekaterinburg

Обоснован сетевой подход к оценке информационных рисков предприятий, которые в условиях формирования сетевых отношений оказывают все большее влияние на операционные и финансовые риски. Авторы описывают последствия информатизации экономики, раскрывают экономические последствия сетезации, угрозы для промышленного предприятия, возникающие в условиях цифровизации. В статье отражены особенности рынка промышленной автоматизации. Описываются некоторые методики по оценке экономической безопасности, которые применимы к промышленному предприятию. Информационные технологии оцениваются как непрерывно развивающиеся, производится оценка рисков для предприятия, которое работает на основе интеллектуального капитала, при наступлении потенциальных информационных угроз.

На основе приведенных результатов исследования по оценке рисков, связанных с деятельностью предприятия, делается предположение, что изменение структуры сетевого промышленного комплекса имеет неоднозначный эффект: с информатизацией экономики увеличивается ущерб, вероятность наступления информационных рисков; делается вывод о взаимосвязи пространственной близости участников промышленной сети с развитием ее свойств. В процессе исследований проведен комплексный анализ состояния системы экономической безопасности промышленного предприятия; выявлены основные проблемы в системе управления информацией, которые оказывают воздействие на уровень экономической безопасности предприятия, а также установлены причины этих проблем. Определена необходимость комплексного решения идентифицированных проблем по управлению информационными угрозами, путем обеспечения информационной, кадровой, технологической, силовой безопасности. Сделан вывод о необходимости функционального распределения ответственности по защите информации в условиях цифровой сетезации промышленности. Определено, что многомерность и разнообразие сетевых отношений в промышленности определяют необходимость в математической формализации, формирование системного сбалансированного подхода к оценке и прогнозированию структурно-пространственных изменений в промышленности.

Таким образом, рассмотрены и уточнены теоретические вопросы, посвященные методическому инструментарию оценки угроз экономической безопасности (в том числе информационных) промышленного предприятия, и получены результаты комплексного анализа классической системы экономической безопасности предприятия. Анализ, систематизация и оценка позволили уточнить специфику цифровой сетезации высокотехнологичного промышленного предприятия, конкретизировать методики, подходящие для данной отрасли по оценке информационных угроз

***Ключевые слова:*** *сетевая экономика; цифровая трансформация; цифровая сетезация; четвертая промышленная революция; информационные риски; информационная безопасность; базы данных; методики оценки; стратегическое управление; экономическая безопасность*

The article substantiates the network approach to the assessment of information risks of enterprises, which have an increasing impact on operational and financial risks. This article describes the effects of economy informatization, also reveals the economic impact of network setting, a threat to industrial enterprises, which arise in the context of digitalisation, moreover, reflected market features industrial automation. It's describes some of the methods of evaluating the economic security that apply to industrial enterprise. Information technologies are assessed as continuously developing assesses risks to the company, which operates based on intellectual capital, upon the occurrence of potential information security threats.

It's based on the results of the study on the assessment of the risks associated with the operations of the company, suggests that the change in the structure of the network industry has an ambiguous effect: with the information economy increases the damage probability of informational risks; concludes the relationship of spatial proximity of the parties to the industrial network with the development of its properties. In the course of studies a comprehensive analysis of the status of economic security system for industrial enterprises was conducted; major problems in information management system, with an impact on the level of economic safety of the enterprise were identified, as well as the causes of these problems. The need for a comprehensive solution to the identified problems on management of information threats, by providing information, personnel, technological, security power was proved. The authors have made a conclusion that there is a functional allocation of responsibility to protect the information in a digital network setting industry. It was determined that multidimensionality and diversity network industrial relations necessitate in mathematical formalization, forming a system of balanced approach to evaluating and forecasting structural-spatial changes in the industry.

Thus, theoretical questions on overall methodological tools assess threats to economic security were reviewed and refined, including information industrial enterprises, and conducted the results of integrated analysis the classical system of economic safety of the enterprise. Analysis, systematization and evaluation clarified the specifics of digital network setting high-tech industrial enterprises; refine techniques suitable for the industry on evaluation of information threats

***Key words:*** *network economy; digital transformation; digital networking; fourth industrial revolution; information risks; information security; database; assessment techniques; strategic management; economic security*

*Введение.* В настоящее время формирование цифровой экономики рассматривается не только с позиций повышения конкурентоспособности российской продукции на мировых рынках в будущем, но и с точки зрения национальной безопасности и безопасности хозяйствующих субъектов. Актуализируются вопросы, связанные с последствиями цифровой сетезации для предприятий, поскольку она имеет широкое распространение во многих смежных отраслях. Риски изменяют свой удельный вес в определении экономической безопасности предприятия – первостепенными становятся факторы, связанные с цифровой сетезацией.

*Объектом исследования* выступают предприятия и организации, активно вовлеченные в информационно-сетевые отношения в процессе создания добавленной стоимости продукта или услуги.

*Предметом исследования* является информационная безопасность компаний, которая в широком смысле включает в себя защиту конфиденциальных сведений, в том числе финансового характера, и производственного процесса от умышленных действий, приводящих к репутационному или финансовому ущербу.

*Цель исследования* – актуализировать проблему информационной безопасности в условиях цифровой сетезации промышленности и обосновать методический инструментарий оценки информационных угроз.

Целесообразно говорить о необходимости формирования методического подхода к обоснованию информационных угроз предприятий и разработке механизмов по управлению ими в условиях формирования цифровых сетевых отношений.

Теоретико-методологическая платформа настоящего исследования основана на комбинации теорий сетевой экономики и экономической безопасности, что позволяет говорить о преобразовании механизмов управления предприятиями в условиях цифровой сетезации промышленности.

*Методология цифровых сетевых отношений.* Едва ли не основным при обосновании эффектов цифровизации является сетевой подход. В теоретическом контексте существуют основные закономерности каталитического процесса распространения цифровых технологий, описываемые зако-

ном Г. Мура и законом Р. Меткалфа. Закон Мура связан со снижающейся во времени стоимостью цифровых коммуникаций [13]. Благодаря данной закономерности, стал возможным стремительный рост цифровых технологий в коммерческом секторе. С точки зрения маркетинга, последствия закона Мура дают уникальную возможность формировать и развивать сетевые отношения между компаниями за счет роста интенсивности и массовости цифровых коммуникаций.

Закон Р. Меткалфа, в свою очередь, показывает связь между количеством пользователей сети и ее ценностью [4] и объясняет, что развитие интернета ведет к росту его общественной ценности. Связь между размером сети и ее ценностью для отдельно взятого предприятия преобразуется в повышение производительности, экономное использование ресурсов и проведение эффективной коммуникационной политики.

На глобальном уровне в ходе информатизации экономики возникает множество информационно-сетевых эффектов, которые можно считать синергетическими. Одновременное действие закона Мура, роста сети Интернет, компьютеризации и новых финансовых инструментов привело к периоду «быстрых инноваций» [3]. В сетевой экономике, по мнению Р. Вайбера, закон убывающей предельной доходности уже не действует. Положительная обратная связь и прямые сетевые эффекты обусловливают возрастающую предельную доходность [2]. Важно отметить, что при этом стремительно масштабируются процессы интеграции и сетизации разработчиков, производителей, продавцов и потребителей информационных благ, а также процессы придания стоимости цифровым сетевым эффектам.

Помимо значительных положительных эффектов цифровая сетезация компаний имеет определенные риски и угрозы. В настоящее время многие компании испытывают потребность в эффективной защите корпоративных систем от угроз информационной безопасности в условиях цифровой экономики.

*Методический инструментарий оценки информационных угроз.* Становится очевидно, что в условиях постоянно меняющихся обстоятельств от руководства требуются решительные действия, которые базируются на непрерывном мониторинге внешних и внутренних угроз цифровой сетезации [9]. Одна из предложенных классификаций угроз включает 9 критериев, которые также соотносятся с рисками, возникающими в условиях сетезации:

1) по месту возникновения: внутренние, внешние;

2) по степени опасности: особенно опасные, опасные;

3) по возможности осуществления: реальные, потенциальные;

4) по масштабу осуществления: локальные, общесистемные;

5) по длительности действия: временные, постоянные;

6) по отношению к ним: объективные, субъективные;

7) по характеру направления: прямые, косвенные;

8) по вероятности наступления: явные, латентные;

9) по природе возникновения: политические, конкурентные.

В условиях информатизации экономики, сетезации промышленных предприятий, остро стоит вопрос применения информационно-коммуникационных технологий (ИКТ) нового поколения [12]. Поскольку в настоящее время защита информации приобретает все большую значимость в сохранении имиджа и конкурентоспособности организации, внедрении автоматизированных инноваций, руководство стремится к следующим эффектам:

– разделение прав доступа к информации;

– защита информации от нежелательного использования;

– стимулирование технологического внедрения в новые сферы при поддержке ИКТ.

Методический инструментарий оценки информационных угроз промышленного предприятия может стать проекцией методов оценки экономической безопасности:

А. В. Шохнех описывает методику оценки нормативов коэффициентов путем поэлементного сравнения групп пассива и актива баланса [1] – это классический метод широкого спектра, применяется в антикризисном управлении, управлении рисками. Данный метод предполагает оценку динамики платежеспособности в различные временные периоды [8];

1) О. Б. Кузнецова описывает количественную методику определения уровня безопасности [1] с помощью моделей вероятности

банкротства (Альтмана, Лиса, Таффлера, Бивера, торгово-посреднической организации);

2) метод экспертных оценок [7] – качественная оценка определения уровня экономической безопасности, широко применимый метод получения информации, интеграции качественных и количественных оценок;

3) экономико-статистический метод [11] – позволяет получить количественную оценку частоты возникновения угроз, масштаб, более широкий список факторов, влияющих на предприятие. Данный метод предполагает сравнение результатов с пороговыми значениями, определение угроз с учетом вероятности возникновения;

4) метод анализа сценариев – процесс математического моделирования трех вероятных сценариев развития компании, оценка инвестиционной привлекательности (NPV) [8].

Базы данных используют для хранения и передачи информации в большинстве структур: промышленная отрасль, государственные органы, коммерческие структуры, отдельные люди. Базы данных, условно сгруппированы по характеру информации: государственные, коммерческие и личностные. Цифровая сетезация позволяет сделать вывод о том, что вероятность наступления внешних и внутренних угроз информационной безопасности предприятия увеличивается.

В аналитической работе коммерческих структур, как правило, присутствует человек, поэтому существует необходимость представления баз данных в таблицах, графиках, так как человеческому мозгу недостаточно текстовой информации (числовые показатели требуют визуализации).

Информационные технологии тесно связаны с промышленными предприятиями: составление базы данных заказчиков, систематизирование технологических процессов, инновационные решения по автоматизации. Таким образом, можно говорить о том, что систематизация информации, автоматизация извлечения необходимых данных, перевод их в базы данных повышают эффективность работы компании. Обмен информацией между промышленными предприятиями ускоряет развитие предприятия благодаря внедрению современных решений.

Однако негативная сторона вопроса проявляется в хищении информации, являющейся коммерческой тайной. Причинами могут являться присвоение клиентской базы, хищение денежных средств, хищение информации с целью получения выкупа, собирание компромата на отдельных людей.

Информационные преступления, связанные с хищением баз данных, условно подразделяются на репутационные и кибернетические. Первый тип ставит под сомнение кадровую безопасность предприятия, второй – информационную, в связи с этим отдел безопасности на предприятии должен выполнять комплексную защиту.

Database Activity Monitoring – аудит и мониторинг баз данных все шире применяется во всем мире, российские банки обязаны использовать такой инструментарий. Также обязательна для использования Data Leak Prevention – контроль действий при доступе к базам данных, блокировка нежелательных действий (копирование информации).

Использование систем защиты не гарантирует сохранность базы данных, во всем мире ежегодно конфиденциальная информация малых, средних и крупных предприятий попадает в руки злоумышленников: данные за 2018 г. по преступлениям в особо крупном размере представлены в табл. 1.

Исходя из оценки экспертов (среднего по численности, выручке инжинирингового предприятия, предлагающего решения по автоматизации производственных процессов), создан реестр рисков (табл. 2) и проведена оценка ущерба и вероятности рисков для коммерческих предприятий РФ. В качестве экспертов выступили руководители названного предприятия: генеральный директор, руководитель отдела продаж, исполнительный директор, технический директор, руководитель отдела комплектации.

В качестве методического инструментария оценки информационных угроз предприятия в условиях цифровой сетезации промышленности целесообразно применить комбинацию метода экспертных опросов (который позволяет учесть специфику деятельности предприятия), метода нечетких множеств (описывает нечеткие понятия и знания, оперировать этими знаниями и делать нечеткие выводы) и матрицы рисков.

Таблица 1 / Table 1

*Похищенные базы данных компаний в особо крупном размере за 2018 г. / Large-scale stolen database of companies for 2018 [10; 15]*

| Страна / Country | Структура / Structure | Ущерб / Damage |
|---|---|---|
| РФ / Russian Federation | ABBYY | Внутренняя документация / Internal documentation |
| | Сбербанк / Sberbank | Персональная информация 420 тыс. сотрудников / Personal information 420 thousand employees |
| Европа / Europe | Ticketfly | 27 млн персональных записей / 27 million personal records |
| | Dixons Carphone | 1,2 млн персональных данных / 1,2 million personal data |
| | Fashion Nexus | 1,3 млн персональных данных / 1,3 million personal data |
| | Veeam Software | 445 млн персональных записей / 445 million personal records |
| | Freeze Pro Shop | 4 млн персональных записей / 4 million personal records |
| Азия / Asia | Careem | 14 млн человек – персональная информация / 14 million people – personal information |
| | SingHealth | Персональная информация 160 тыс. человек / Personal information 160 thousand people |
| | Timehop | 21 млн персональных данных / 21 million personal data |
| | Huazhu Hotels Group | Персональные данные 130 млн человек / Personal data 130 million people |
| | Alibaba Group | 10 млн персональных записей / 10 million personal records |
| | Nixi Technology | Персональные данные 5.3 млн пользователей / Personal data 5,3 million users |
| США / USA | Under Armour | 150 млн персональных данных / 150 million personal data |
| | Orbitz | Около 880 тыс. банковских карт / About 880 thousand bank cards |
| | MBM Company Inc | Персональная информация 1,3 млн человек / Personal information 1,3 million people |
| | Delta Air Lines, Best Buy и Sears Holding Corp. | Банковская информация 100 тыс. банковских карт / Banking information 100 thousand bank cards |
| | Saks, Lord & Taylor | Более 5 млн банковских карт / Over 5 million bank cards |
| | Exactis | 230 млн персональных данных, 110 млн данных организаций / 230 million personal data, 110 million data organizations |
| | Sacramento Bee | 19,4 млн записей с персональными данными / 19,4 million records with personal data |
| | T-Mobile | 2 млн счетов американского сотового оператора / 2 million accounts of the American mobile operator |
| | Facebook | Данные 50 млн аккаунтов / Data 50 million accounts |
| | Google | Данные 52,5 млн пользователей / Data of 52,5 million users |
| | American Express India | Данные 2,3 млн клиентов / Data 2.3 million customers |
| | Marriott | 327 млн банковская информация /327 million banking information |
| | Data & Leads | 60 млн персональных записей /60 million personal records |
| Канада / Canada | Level One Robotics and Controls | Коммерческая информация и банковская информация / Commercial information and banking information. |
| Израиль / Israel | MyHeritage | 92 млн записей персональной информации / 92 million personal information records |

Таблица 2 / Table 2

*Риски от хищения баз данных для предприятия, баллов / Enterprise database theft risks, points*

| **Экономические / Economic** | **Социальные / Social** | **Коммерческие / Commercial** | **Профессиональные / Professional** |
|---|---|---|---|
| Увеличение издержек – 6 / Cost increase – 6 | Нарушение имиджа сотрудников – 5 / Violation of the image of employees – 5 | Банкротство – 14 / Bankruptcy – 14 | Утечка внутренней информации – 13 / Leak of internal information – 13 |
| Снижение конкурентоспособности – 12 / Decrease in competitiveness – 12 | | Потеря платежеспособности – 15 / Loss of solvency – 15 | Уход ведущих специалистов компании – 10 / Leaving leading company specialists – 10 |
| Нарушение имиджа компании – 11 / Violation of the company's image – 11 | | | |

Широко применимый метод нечетких множеств, используемый в антикризисном управлении, оценке рисков, в технической сфере, следует считать актуальным в условиях цифровой сетезации. Подход перехода из имеющихся количественных и качественных данных в количественные значения показателей ввел Лотфи Заде в 1965 г. [14]. Для определения количественного показателя из метода экспертного опроса необходимо применять формулу [3]

$$pr = U \times P \ , \qquad (1)$$

где pr – значимость показателя;

U – ущерб;

P – вероятность.

Для определения сводного значения риска используется формула [5]

$$Pr = (U1 \times P1 + U2 \times P2 + U3 \times P3 + \\ + U4 \times P4 + \ldots + Un \times Pn)/n \ , \qquad (2)$$

где r – сводное значение значимости показателя;

P – вероятность;

U – ущерб;

n – количество экспертов.

На основе полученных данных, представленных в табл. 2, построена матрица рисков (табл. 3).

Таблица 3 / Table 3

*Матрица рисков, баллов / Risk matrix, points*

| Вероятность / Probability | | | | |
|---|---|---|---|---|
| | 12 / 12 (2) | 13 / 13 (7) | *15 / 15 (6)* | *16 / 16* |
| | 9 / 9 | 10 10 (8) | 11 / 11 (3) | *14 / 14 (5)* |
| | *3 / 3* | 6 /6 (1) | 7 / 7 | 8 /8 |
| | *1 / 1* | *2 /2* | 4 /4 | 5 /5 (4) |
| Ущерб / Damage | | | | |

Следует отметить, что градация рисков произведена следующим образом: 1…3 балла – очень низкий риск (0…19 %) (в таблице выделен курсивом в левом нижнем углу); 5…8 баллов – низкий риск (20…50 %); 9…13 баллов – средний риск (51…80 %); 14…16 баллов – высокий риск (81…100 %) (в таблице выделен курсивом в правом верхнем углу).

Очевидно, что информационные угрозы предприятия в условиях цифровой сетезации, в первую очередь, влияют на коммерческие риски. Остальные риски попадают в «желтую зону».

Предприятие, которое стремится защитить информацию, должно иметь либо структурное подразделение – отдел безопасности, комплексно идентифицирующий и минимизирующий все риски, поскольку они имеют явные и неявные причинно-следственные связи, либо передавать функции по мониторингу среды на аутсорсинг.

При комплексном подходе необходимо обратиться к трехуровневой защите предприятия. Первый уровень включает отделы информационных технологий, отделы информационной безопасности и другие подразделения, отвечающие за идентификацию информационных угроз. Второй уровень защиты – это отделы управления рисками, имеющие дело не только с технической стороной информационных рисков, но и с их влиянием на все экономические процессы компании. Третий уровень защиты – это отделы внутреннего аудита и контроля, которые проводят оценку влияния информационных рисков на финансовые показатели компании.

*Заключение.* Цифровое преобразование экономической системы со значительным количеством сетевых вертикальных и горизонтальных связей является достаточно продолжительным процессом, имеющим как положительные, так и отрицательные последствия. Угрозы информационной безопасности компаний, приводящие к финансовым и репутационным потерям, требуют перехода к проактивной защите, которая достигается путем адекватной оценки информационных рисков. Исследование показало, что данная группа рисков в условиях цифровой сетезации напрямую влияет на операционные риски компаний, а механизм управления ими является комплексным и многоуровневым.

**Список литературы**

1. Асадова А. А. Количественные методы оценки экономической безопасности предприятия // Теория и практика сервиса: экономика, социальная сфера, технологии. 2017. № 3. С. 32–36.

2. Вайбер Р. Эмпирические законы сетевой экономики // Проблемы теории и практики управления. 2003. № 3. С. 86–91; № 4. С. 82–88.

3. Вэриан Х. Р. Экономическая теория информационных технологий // Социально-экономические проблемы информационного общества. Сумы: Университетская книга, 2005. С. 214–276.

4. Дятлов С. А. Сетевые эффекты и возрастающая отдача в информационно-инновационной экономике // Известия Санкт-Петербургского государственного экономического университета. 2014. № 2. С. 7–11.

5. Ишкильдина С. А., Вишняков М. А., Щипанов В. В., Соколова Л. Р., Карсунцева А. А. Методика анализа рисков в процессах производства // Известия Самарского научного центра РАН. 2016. Т. 18, № 4. С. 31–39.

6. Калиновская С. Ю. Методика интегральной оценки риска инновационного проекта // Инновации. 2015. № 2. С. 107–110.

7. Макарова И. Л. Анализ методов определения весовых коэффициентов в интегральном показателе общественного здоровья // Символ науки. 2015. № 7. С. 87–95.

8. Манушин Д. В. Уточнение понятия и структуры методологии антикризисного управления и методологии антикризисного управления макроэкономикой // Актуальные проблемы экономики и права. 2018. № 2. С. 46–49.

9. Самочкин В. Н., Барахов В. И. Экономическая безопасность промышленных предприятий // Известия Тульского государственного университета. Экономические и юридические науки. 2014. № 3-1. С. 342–352.

10. Степанов И. Сравнительный обзор средств предотвращения утечек данных (DLP). URL: https://www.safe-surf.ru/specialists/article/5233/609990 (дата обращения: 18.03.2019). Текст: электронный.

11. Хиревич Э. Ю. Определение оптимальной методики оценки экономической безопасности предприятия // Инновационная наука. 2016. № 2-2. С. 123–127.

12. Щукина Л. В. Теоретические аспекты устойчивого развития региональных социально-экономических систем // Псковский регионологический журнал. 2015. № 21. С. 38–50.

13. Moore G. E. Cramming more components onto integrated circuits // Electronics. 1965. Vol. 38, No. 8. P. 114–117.

14. Roberts S. Remembering Lotfi Zadeh, the inventor of fuzzy logic. URL: https://www.newyorker.com/tech/annals-of-technology/remembering-lotfi-zadeh-the-inventor-of-fuzzy-logic (дата обращения: 09.03.2019). Текст: электронный.

15. Salim S. Revealed: the 21 biggest data breaches of 2018 (Digital information world). URL: https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12 (дата обращения: 11.07.2019). Текст: электронный.

**References**

1. Asadova A. A. *Teoriya i praktika servisa: ekonomika, sotsialnaya sfera, tehnologii* (Theory and practice of service: economics, social sphere, technologies), 2017, no. 3, pp. 32–36.

2. Viber R. *Problemy teorii i praktiki upravleniya* (Problems of theory and practice of management), 2003, no. 3, pp. 86–91; no. 4, pp. 82–88.

3. Varian H. R. *Sotsialno-ekonomicheskie problemy informatsionnogo obshchestva* (Socio-economic problems of the information society), Sumy: University Book, 2005, pp. 214–276.

4. Dyatlov S. A. *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta* (News of St. Petersburg State University of Economics), 2014, no. 2, pp. 7–11.

5. Ishkildina S. A., Vishnyakov M. A., Shchipanov V. V., Sokolova L. R., Karsuntseva A. A. *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta* (Bulletin of the Samara Scientific Center of the Russian Academy of Sciences), 2016, vol. 18, no. 4, pp. 31–39.

6. Kalinovskaya S. Yu. *Innovatsii* (Innovations), 2015, no 2, pp. 107–110.

7. Makarova I. L. *Simvol nauki* (Symbol of science), 2015, no. 7, pp. 87–95.

8. Manushin D. V. *Aktualnye problemy ekonomiki i prava* (Actual problems of economics and law), 2018, no. 2, pp. 46–49.

9. Samochkin V. N., Barakhov V. I. *Izvestiya Tulskogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki* (Bulletin of the Tula State University. Economic and legal sciences), 2014, no. 3–1, pp. 342–352.

10. Stepanov I. *Sravnitelny obzor sredstv predotvrashcheniya utechek dannyh (DLP)* (Comparative review of means of data leakage prevention (DLP)). URL: https://www.safe-surf.ru/specialists/article/5233/609990 (Date of access: 18.03.2019). Text: electronic.

11. Khirevich E. Yu. *Innovatsionnaya nauka* (Innovation Science), 2016, no. 2–2, pp. 123–127.

12. Schukina L. V. *Pskovskiy regionologicheskiy zhurnal* (Pskov Regional Journal), 2015, no. 21, pp. 38–50.

13. Moore G. E. *Electronics* (Electronics), 1965, vol. 38, no. 8, pp. 114–117.

14. Roberts S. *Remembering Lotfi Zadeh, the inventor of fuzzy logic* (Remembering Lotfi Zadeh, the inventor of fuzzy logic). URL: https://www.newyorker.com/tech/annals-of-technology/remembering-lotfi-zadeh-the-inventor-of-fuzzy-logic (Date of access: 09.03.2019). Text: electronic.

15. Salim S. Revealed: the 21 biggest data breaches of 2018 (Digital information world) (Revealed: the 21 biggest data breaches of 2018 (Digital information world)). URL: https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12 (Date of access: 11.07.2019). Text: electronic.

Статья подготовлена при финансовой поддержке гранта РФФИ № 18-010-01156 «Моделирование технологической трансформации промышленного комплекса России в условиях цифровизации экономики»

**Коротко об авторах**

*Акбердина Виктория Викторовна,* д-р экон. наук, профессор РАН, заведующая отделом региональной промышленной политики и экономической безопасности, Институт экономики Уральского отделения РАН, профессор, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург, Россия. Область научных интересов: сетевой промышленный комплекс, цифровизация промышленности, экономическая безопасность, инновационно-технологическое развитие, промышленная политика
akb_vic@mail.ru

*Невская Анастасия Дмитриевна,* аспирант, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург, Россия. Область научных интересов: сетевой промышленный комплекс, цифровизация промышленности
tikhonova.nastiya@mail.ru

**Briefly about the authors**

*Victoria Akberdina,* doctor of economics, professor RAS, head of the Regional Industrial Policy and Economic Security department, Institute of Economics, Ural branch of RAS, Professor of Ural Federal University named after. B. N. Yeltsin, Ekaterinburg, Russia. Sphere of scientific interests: network industrial complex, digitalization of industry, economic security, innovation and technological development, industrial policy

*Nevskaya Anastasia,* postgraduate, Ural Federal University named after the first President of Russia B. N. Yeltsin, Yekaterinburg, Russia. Sphere of scientific interests: network industrial complex, digitalization of industry, economic security, innovation and technological development, industrial policy

**Образец цитирования**

*Акбердина В. В., Невская А. Д. Информационные угрозы в условиях цифровой сетезации: методический инструментарий оценки и механизм управления // Вестник Забайкальского государственного университета. 2019. Т. 25, № 9. С. 105–113. DOI: 10.21209/2227-9245-2019-25-9-105-113.*

*Akberdina V., Nevskaya A. Information threats in digital networks: methodological tools, assessments and management mechanism // Transbaikal State University Journal, 2019, vol. 25, no. 9, pp. 105–113. DOI: 10.21209/2227-9245-2019-25-9-105-113.*

Статья поступила в редакцию: 10.07.2019 г.
Статья принята к публикации: 18.11.2019 г.