УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ПЕРЕХОДА К ЦИФРОВОМУ ПРОИЗВОДСТВУ

[1]Подлевских А.П., [2]Прохончуков С.Р., [1]Ретюнских С.Н.

[1]ГКОУ ВО «Российская таможенная академия», Люберцы;

[2]АО «Специализированное конструкторско-технологическое бюро электронных систем», Воронеж, e-mail: APodlevskikh7@yandex.ru, sprokhonchukov@gmail.com, s.retyunskih@customs-academy.ru

В статье рассматриваются и обосновываются решения, направленные на повышение уровня информационной безопасности в условиях перехода к цифровому производству. Рассмотрена и дополнена классификация основных средств информационной безопасности (ИБ) применительно к условиям организации цифрового производства. Перспективным направлением, по мнению авторов, является построение «цифрового прототипа» предприятия или производства, который позволит спроектировать виртуальную копию реального объекта (системы), исследовать его производственные и технологические процессы, информационную безопасность, определить оптимальные параметры, узкие места, провести анализ различных сценариев работы производственной системы «AS IS» и «TO BE», не создавая при этом риски вмешательства в реальный процесс (систему). Анализ публикаций по тематике исследования позволил определить основные направления и перспективы ИБ для цифрового производства с учетом имеющегося уровня автоматизированных систем управления технологическими процессами (АСУТП). Осуществление перехода к цифровым предприятиям предлагается через промежуточные модели, ориентированные на центры компетенций, которые в свою очередь базируются на элементах цифровой архитектуры производства с учетом специфики отрасли. Авторы предполагают, что для реализации центров компетенций информационной безопасности (ЦКИБ) наиболее подходящими являются модели «Консорциум потребителей» и «Головной поставщик». Реализация аутсорсинга ИБ на первых этапах перехода к цифровому производству позволит обеспечить и реализовать конкурентное преимущество за счет моделирования и прогнозирования перспективных моделей перехода к цифровому производству (ЦП). Экономический эффект от моделирования, прогнозирования, разработки моделей ИБ для ЦП с учетом концепции «Индустрия 4.0», а также подготовка кадров с учётом перспектив в направлении ИБ позволят оптимизировать затраты и обеспечить повышение эффективности производства на 12–20%.

Ключевые слова: цифровое производство, информационная безопасность, защита информации в сетях и автоматизированных системах, платформа единого цифрового пространства, правовые и технологические риски, модели сорсинга, индустриальная автоматизация

ENSURING INFORMATION SECURITY IN THE TRANSITION TO DIGITAL PRODUCTION

[1]Podlevskikh A.P., [2]Prokhonchukov S.R., [1]Retyunskikh S.N.

[1]Russian Customs Academy, Lyubertsy;

[2]Joint Stock Company (JSC) Specialized Design and Technology Bureau of Electronic System, Voronezh, e-mail: APodlevskikh7@yandex.ru, sprokhonchukov@gmail.com, s.retyunskih@customs-academy.ru

The article discusses and justifies solutions aimed at improving the level of information security in the context of the transition to digital production. The classification of the main means of information security (IS) in relation to the conditions of the organization of digital production is considered and supplemented. A promising direction, according to the authors, is the construction of a «digital prototype» of an enterprise or production, which will allow you to design a virtual copy of a real object (system), investigate its production and technological processes, information security, determine the optimal parameters, bottlenecks, analyze various scenarios of the production system «AS IS» and «TO BE», without creating risks of interference in the real process (system). The analysis of publications on the subject of the study allowed us to determine the main directions and prospects of information security for digital production, taking into account the existing level of automated process control systems (APCs). The implementation of the transition to digital enterprises is proposed through intermediate models focused on competence centers, which in turn are based on elements of the digital production architecture, taking into account the specifics of the industry. The authors suggest that the «Consortium of Consumers» and «Head Supplier» models are the most suitable for the implementation of information security competence centers. The implementation of information security outsourcing at the first stages of the transition to digital production will ensure and realize a competitive advantage by modeling and predicting promising models of the transition to digital production (CP). The economic effect of the modeling, forecasting, modelling IB CPU given the concept of «industry 4.0», as well as training from the perspectives of in the direction of IB will allow to optimize costs and improve production efficiency by 12-20%.

Keywords: digital production, information security, information protection in networks and automated systems, the platform of a single digital space, legal and technological risks, sourcing models, industrial automation

Современность и перспектива развития промышленности требуют детального и всестороннего рассмотрения вопроса информационной безопасности в условиях организации ЦП. Важность и необходимость обусловлены тем, что особенностью четвертой промышленной революции является комплектование производства гибкими мо-

дульными автоматизированными системами и промышленными роботами.

По мнению экспертов, ущерб от киберпреступлений от года к году возрастает в геометрической прогрессии, и если сумма убытков в 2018 г. составила около 2,7 млрд долларов, то к 2022 г. она может составить уже свыше 8 млрд долларов [1; 2].

Трудно представить, что конвейер предприятия с использованием цифрового производства по выпуску лекарств или средств защиты вышел из строя по причине внутренней ошибки или из-за внешней кибератаки. Такие остановки производства могут привести к необратимым и высокозатратным, с экономической точки зрения, последствиям.

Любые внешние или внутренние атаки на автоматизированную систему производства должны быть локализованы и устранены без явных угроз производству. Киберугроза, как незаконное проникновение в единое цифровое пространство производства, должна быть полностью исключена.

Предполагается, что в условиях цифрового производства средства и системы обеспечения информационной безопасности должны обладать свойствами к самообучению с элементами искусственного интеллекта (ИИ).

Цель исследования состоит в том, чтобы в рамках научного и учебно–исследовательского процесса рассмотреть информационную безопасность при реализации и организции цифрового производства.

Материалы и методы исследования

В основу исследований авторами предложен системный и функциональный анализ.

Потребности современного рынка меняются в зависимости от политических, экономических и частных взглядов той или иной группы потребителей. В общей сложности производитель направляет на рынок тот товар или услугу, на которые имеется спрос. Информационная модель, описывающая взаимоотношения всех участников рынка, должна быть максимально адекватной, чтобы обеспечить высокую эффективность прогнозирования и удовлетворения спроса [3]. Необходимо отметить, что адекватная информационная модель должна учитывать все характеристики предоставляемых продуктов и услуг, что обеспечивается за счет тщательной проработки всех операций и состава ресурсов технологического процесса. В целом цифровое производство, организованное в условиях промышленного предприятия, представлено комплексом всевозможных синхронизированных между собой моделей: информационных, математических, логических и т.п., основная цель которых – обеспечить понимание и контроль процессов на всех управленческих и технологических уровнях [4; 5].

Перспективным направлением, по мнению авторов, является построение «цифрового прототипа» предприятия или производства, который позволит спроектировать виртуальную копию реального объекта (системы), исследовать его производственные и технологические процессы, информационную безопасность, определить оптимальные параметры, узкие места, провести анализ различных сценариев работы производственной системы «AS IS» и «TO BE», не создавая при этом риски вмешательства в реальный процесс (систему).

В настоящее время переход к модели цифрового производства требует детальной проработки и проведения анализа имеющегося производственного и управленческого потенциала. Не всегда возможно осуществить переход к новой модели производства и/или управления за один этап, известны случаи, когда переход к новой модели организуют через промежуточные этапы.

В качестве переходной модели (рис. 1) предлагается обеспечить и/или использовать ранее организованные, интегрированные в производство автоматизированные линии, системы управления производственными процессами [6], системы автоматизации разработки технологической документации и др. Учитывая, что на разных предприятиях одной и той же промышленности могут применяться абсолютно разные средства автоматизации (CAD, CAM, PDM, CRM, ERP и др.), первой необходимостью является создание такого единого цифрового пространства, которое обеспечит однозначное понимание всех информационных сообщений участниками цифрового производства. Конечно, вопрос импортозамещения остается открытым, поскольку отечественное программное обеспечение (ПО) может снизить риски от непредвиденных ситуаций с запретом разработчиков на применение импортного ПО.

В этой связи для осуществления перехода к цифровой модели производства было бы правильно создать отечественный программно-аппаратный комплекс, который бы отвечал требованиям отечественных стандартов и учитывал специфику подобных зарубежных комплексов. Кроме того, по мнению авторов, одним из важнейших аспектов развития предприятий цифрового производства является обеспечение комплексной информационной безопасности.

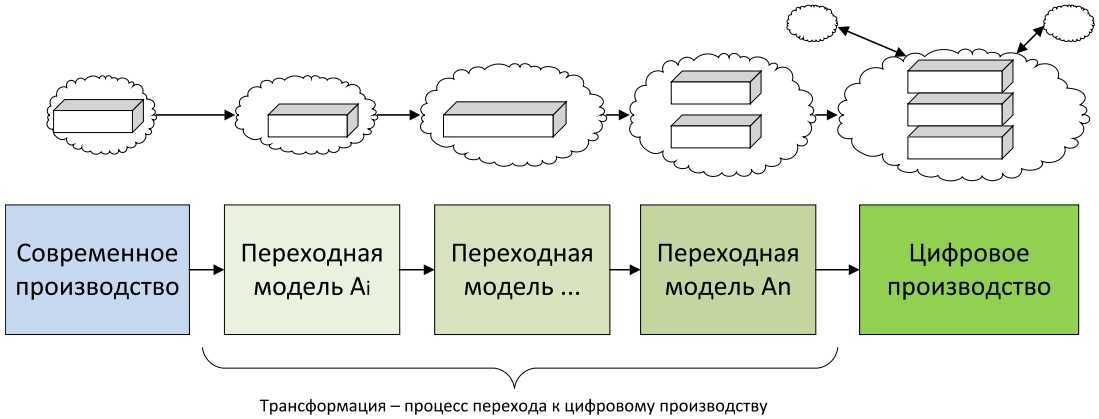


Рис. 1. Схема перехода от современного к цифровому производству

Таким образом, разработанные подробные обеспечивающие модели цифрового производства позволят определять причины внутренних ошибок при функционировании системы, а также сформировать карту потенциальных уязвимостей для разработки мероприятий по предотвращению возможных киберугроз.

Уровень автоматизации и роботизации производства различный и зависит от сектора экономики. Рассмотрим предприятия машиностроения, поскольку создание основных средств производства является одной из актуальных задач любого государства. Производство машиностроения может быть представлено наличием автоматизированных систем управления технологическими процессами (АСУТП) или роботизированных комплексов [6; 7]. Для обеспечения корректного перехода к цифровому производству необходимо определить особенности требований к информационной безопасности АСУТП:

– организация и управление сложными техническими объектами;

– работа в системе реального времени;

– минимизация времени на реакцию технологических и управленческих систем;

– отсутствие единого цифрового пространства [8].

Современные условия диктуют свои требования, которые необходимо учесть при построении переходных моделей к цифровому производству. Административные и программно-технические меры обеспечения ИБ АСУТП являются взаимодополняющими направлениями. Однако необходимо отметить, что при реализации модели цифрового производства, по всей видимости, будут применяться программно-аппаратные комплексы различных производителей, поэтому это необходимо учесть в концепции реализации ЦП.

Основной трудностью в реализации информационной безопасности на промышленном предприятии является сложность в разработке и внедрении платформы для единого цифрового пространства. На сегодня по большей степени эта среда взаимодействия представлена сетью Интернет, что, в свою очередь, требует от систем ИБ высоких показателей, которые, в свою очередь, являются очень затратными [4; 9].

По мнению авторов, единое цифровое пространство необходимо выстроить на платформе, которая представлена системой, объединяющей бизнес–процессы на различных предприятиях и в отрасли в целом. Модель информационной безопасности цифрового производства должна строиться с учетом следующих требований к развитию платформы единого цифрового пространства (рис. 2) [9].

Рис. 2. Общие требования к платформе единого цифрового пространства для организации ЦП

1. Компактность и простота использования – автоматизация и роботизация работы с большим объемом данных (Big Data, IoT,

Blockchain) на всех уровнях архитектуры цифрового производства.

2. Сбалансированность – свойство соблюдения баланса по всем системам цифрового производства, в том числе и в межотраслевых связях.

3. Эпистемологичность – свойство платформы единого цифрового пространства соответствовать стратегии развития, планируемым целям и задачам.

4. Безопасность – обеспечение информационной безопасности единого цифрового пространства платформы ЦП, при котором обеспечивается защищенность от внешних и внутренних угроз.

5. Динамичность – свойство единого цифрового пространства платформы ЦП, при котором обмен данными происходит в режиме реального времени по прямым и обратным связям всех механизмов, что позволяет повысить чувствительность в работе ЦП.

6. Универсальность платформы единого цифрового пространства, как предлагается авторами, представляет собой возможность платформы в режиме реального времени проводить изменения в структуре и свойстве элементов без остановки процессов на цифровом производстве. Подразумевается, что часть объемов производства будет перераспределена на смежные цифровые предприятия, что позволит оперативно переналадить производственную линию [10–12].

По мнению авторов, переход к цифровому производству требует изучения и снижения рисков не только в ИБ, но и в других направлениях: политических, финансово-экономических, правовых, технологических, управленческих, социальных [13–15].

Далее в рамках цифрового предприятия более подробно рассмотрим технологические и правовые риски.

Технологические риски, как и риски информационной безопасности, позволяют оценить уязвимости системы и выделить несовершенство внедряемых новых технологий [13], например:

– заимствованные технологии, сервисы, программное обеспечение;

– киберпреступность и электронный шпионаж;

– утечка данных;

– возможные уязвимости новых цифровых технологий цифровой экономики (BigData, IoT, Blockchain);

– расширение проникновения информационных систем в системы государственного и военного управления;

– передача функции принятия решений от человека к ИИ и др.

Риски правового характера при реализации системы ИБ для организации цифрового производства, прежде всего, будут проявляться в неопределенности законодательства, регулирующего деятельность в виртуальном пространстве. Для снижения рисков в области права необходимо уже сегодня прорабатывать и принимать нормативно–правовые документы, направленные на пресечение роста мошенничества и коррупционных действий в едином цифровом пространстве цифрового производства. Кроме того, существует ряд вопросов, которые требуют детального рассмотрения и связаны с трудовыми отношениями и статусом компании, входящей в комплекс цифрового производства. Например [13]:

– юридическая неопределенность ответственности субъектов правоотношений при организации цифрового производства;

– отставание нормативно-правового регулирования экономических отношений в «виртуальном пространстве» от скорости «цифровизации»;

– регуляторные проблемы, обеспечение юридической значимости технологий цифровой экономики и цифрового производства;

– неопределенность правового статуса трудовых отношений в цифровой среде;

– отсутствие правового механизма контроля и надзора соответствия установленным требованиям;

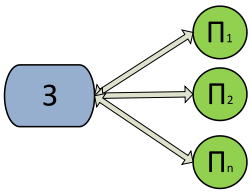
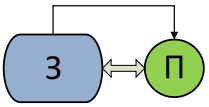
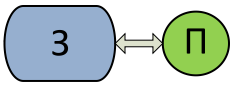
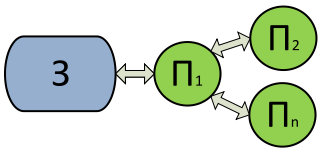
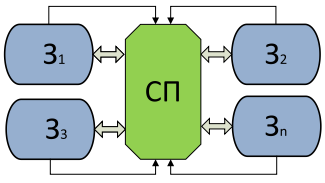
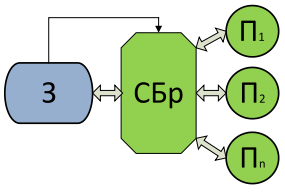
– отсутствие правового управления регулирования деятельности коммерческих организаций по сбору, передаче, хранению и обработке цифровых данных субъекта и др.

Для обеспечения ИБ при трансформации современного производства к ЦП (рис. 1) авторы предполагают, что создание профильных центров компетенций обеспечит высокий уровень проводимых работ и концентрацию высококвалифицированных специалистов на стратегически важных направлениях.

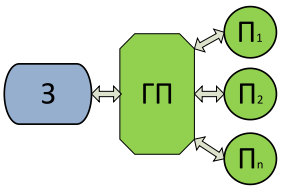
Например, создание центра компетенций ИБ (ЦКИБ) для цифрового производства в машиностроении позволит накапливать знания и реализовывать их в рамках единого цифрового пространства отрасли или комплекса предприятий [16]. После разрешения правовых рисков и вопросов для ЦП отношения между предприятиями и ЦКИБ можно будет выстраивать по следующим моделям (таблица) [17].

По мнению авторов, при обеспечении информационной безопасности центрами компетенций для переходных моделей к цифровому предприятию наиболее подходящими являются модели «Консорциум потребителей», «Сервисный бренд» и «Головной поставщик».

Модели сорсинга ИБ для центров компетенций в условиях перехода от современного к цифровому производству

№ п/п	Модель сорсинга ИБ (графическая модель)	Описание	Достоинства	Недостатки
1	Внутренний поставщик  З – заказчик; П – поставщик	Подразделение компании обеспечивает ИБ (ИТ или ИБ – служба)	Гибкость при реализации проектов ИБ. Оперативность выполнения работ	Ограничения в масштабах, знаниях, доступности к ресурсам и внешнему рынку
2	Мультисорсинг 	Селективный (выборочный) аутсорсинг ИБ	Надёжность за счет распределения контрактов на оказание услуг ИБ и выбор лучшего аутсорсера	Сложности с ведением документации. Высокие риски при выстраивании работы по ИБ
3	Инсорсинг 	Служба ИБ – в качестве отдельной бизнес-единицы	Оказание услуги ИБ на основе некоторых введенных бизнес-правил (относительно формальные контракты, SLA, определение стоимости услуг). Высокая степень автономности	Ограниченность в масштабах знаний и доступа к инновационным ресурсам. Низкая степень контроля утечки информации. Ответственность на заказчике
4	Полный аутсорсинг 	Заключение контракта с единственным поставщиком (ESP) на все услуги ИБ	Перекрытие большей части потребностей компании в услугах ИБ. Стратегическое партнерство топ-менеджмента компании с поставщиком. Заключение долговременных (на срок 5–10 лет) контрактов	Низкая степень автономности ИБ заказчика. Высокие риски утечки информации. Ответственность в равных долях, но чаще всего на поставщике
5	Консорциум: а) консорциум лучших  б) консорциум потребителей  СП – совместное предприятие	Создается для полного аутсорсинга ИБ по крупным государственным контрактам и/или проектам единичных интернациональных компаний	Большие объемы. Доступность к инновационным технологиям. Кооперация	Сложность в реализации. Высокие требования к уровню компании и квалификации сотрудников ИБ
6	Сервисный бренд  СБр – сервисный бренд	Компания создается для предоставления услуг большой организации или группе компаний	Создается под определённую компанию с последующим выходом на внешний рынок	Ограничения в ресурсах и времени. Зависимость от инновационных технологий

Окончание таблицы

№ п/п	Модель сорсинга ИБ (графическая модель)	Описание	Достоинства	Недостатки
7	Головной поставщик  ГП – головной поставщик	Управление и интеграция возможностей различных поставщиков услуг ИБ с целью наследования возможности предоставления услуг ИБ заказчику	Снижение стоимости услуг за счет массовости процессов. Стандартизация процессов ИБ	Высокая зависимость от внешних факторов и поставщика

Заключение

Будущее за цифровыми технологиями [2; 14; 18]. Корректно сформулированная и принятая концепция перехода от современного производства к ЦП позволит оптимизировать затраты и обеспечить преимущество в долгосрочной перспективе. Осуществление перехода к цифровым предприятиям предлагается через промежуточные модели, ориентированные на центры компетенций, которые в свою очередь базируются на элементах цифровой архитектуры производства с учетом специфики отрасли. Многие вопросы ЦП еще требуют детального рассмотрения (правовые, управленческие, ИБ и др.). Однако вопросы информационной безопасности необходимо прорабатывать уже сегодня, что позволит снизить риски в работе всех механизмов ЦП. Цифровое производство подразумевает общее пространство для предприятий отрасли и сектора экономики, поэтому модель сорсинга ИБ должна быть адекватной ситуации и эффективной. По мнению авторов, работа предприятий ЦП в будущем будет представлять общий комплекс, увязанный на платформе единого цифрового пространства, что в свою очередь потребует от центров компетенций высоких показателей эффективности функционирования.

Экономический эффект от моделирования, прогнозирования, разработки моделей ИБ для ЦП с учетом концепции «Индустрия 4.0», а также подготовка кадров с учётом перспектив в направлении ИБ позволит оптимизировать затраты и обеспечить повышение эффективности производства на 12–20 %.

Список литературы

1. Почти 80% российских компаний столкнулись с кибератаками в 2019 году. COMNEWS. Новости цифровой трансформации, телекоммуникаций, вещания и ИТ [Электронный ресурс]. URL: https://www.comnews.ru/digital-economy/content/203714/2019-12-23/2019-w52/pochti-80-rossiyskikh-kompaniy-stolknulis-kiberatakami-2019-godu (дата обращения: 01.02.2021).

2. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. № 2 (26). С. 2–15.

3. Фролов А.Л. Специфика экономического анализа инновационных проектов // Экономический анализ: теория и практика. 2013. № 1. С. 25–31.

4. Николаевский В.В., Рудковская О.Г. Нелинейная динамика развития и проектный подход в методологии стратегического планирования // Научные исследования экономического факультета. Электронный журнал. 2018. Т. 10. № 3(29). С. 7–26.

5. Зеленков Ю.А. Гибкая корпоративная информационная система: концептуальная модель, принципы проектирования и количественные метрики // Бизнес-информатика. 2018. № 2 (44). С. 30–44.

6. Иванов А.А. Автоматизация технологических процессов и производств: учебное пособие для вузов по специальности «Автоматизация технологических процессов и производств (машиностроение)» (направление «Автоматизированные технологии и производства») и направлению «Конструкторско-технологическое обеспечение машиностроительных производств». 2-е изд., испр. и доп. М.: Форум, ИНФРА-М, 2015. 223 с.

7. Прохончуков С.Р., Подлевских А.П. Повышение эффективности распределения пропускной способности магистрали сети автоматизированной системы управления между гибкими производственными модулями // Фундаментальные исследования. 2014. № 11–4. С. 783–792.

8. Андреев Ю.С., Дергачев А.М., Жаров Ф.А., Садырин Д.С. Информационная безопасность автоматизированных систем управления технологическими процессами // Изв. вузов. Приборостроение. 2019. Т. 62. № 4. С. 331–339.

9. Евтянова Д.В. Критерии создания цифровых платформ управления экономикой // Экономические системы. 2017. Т. 10. № 3(38). С. 54–57.

10. Ряполова Е.И., Шрейдер М.Ю., Боровский А.С. Метод обработки информации для поддержки принятия решений в управлении облачным сервисом // Вопросы кибербезопасности. 2018. № 3 (27). С. 39–46.

11. Кудрявцев Д.В., Зараменских Е.П., Арзуманян М.Ю. Разработка учебной методологии управления архитектурой предприятия // Открытое образование. 2017. Т. 21. № 4. С. 84-92.

12. Прохончуков С.Р., Подлевских А.П., Квасова Е.Н. Коммуникационный уровень распределенной системы управления гибкими производственными модулями // Современные проблемы науки и образования. 2015. № 1–1. [Электронный ресурс]. URL: http://science-education.ru/ru/article/view?id=18705 (дата обращения: 10.02.2021).

13. Графова Т.О., Шаповалов А.Ф. Риски и угрозы экономической безопасности в цифровой экономике // Азимут научных исследований: экономика и управление. 2020. Т. 9. № 1(30). С.382–386.

14. Подлевских А.П., Фролов А.Л. Экономическая оценка обоснованности выбора инновационного проекта // Международный журнал прикладных и фундаментальных исследований. 2015. № 12–7. С. 1287–1292.

15. Ретюнских С.Н. Направления реализации в таможенных органах доктрины информационной безопасности Российской Федерации // Цифровая таможня и «Единое окно»: тренды и содержание: сборник материалов научно-практической конференции. Люберцы: ГКОУ ВО «Российская таможенная академия», 2017. С. 47–53.

16. Прохончуков С.Р., Подлевских А.П., Методология написания магистерских диссертаций студентами направлений «Информатика и вычислительная техника» // Образовательная среда сегодня и завтра: сборник научных трудов IX Международной научно-практической конференции / Под общ. ред. Г.Г. Бубнова, Е.В. Плужника, В.И. Солдаткина. 2014. С. 84-89.

17. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография / Под общ. ред. С.Ф. Боева. СПб.: Издательский Дом «Афина», 2017. 440 с.

18. Ретюнских С.Н. Анализ стратегии развития информационного общества в Российской Федерации на 2017–2030 годы // Аллея науки. 2018. Т. 1. № 8(24). С. 596–602.