МАТЕМАТИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ МОДЕЛИРОВАНИЯ И ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ В ЭКОНОМИКЕ, ТЕХНИКЕ И УПРАВЛЕНИИ

УДК 33.338.2 DOI:10.34708/GSTOU.CONF.2020.33.63.002

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ УГРОЗ БИЗНЕС-ПРОЦЕССА КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

Мясоедов А.И.
ФГБОУ ВО «Московский государственный психолого-педагогический университет», г. Москва, Россия

В статье рассматривается представление одного из возможных вариантов выбора стратегии информационной безопасности бизнес-процесса коммерческой организации, посредством комбинаторного подбора факторов математической модели минимально-достаточного уровня защищенности информационных активов организации для противостояния угрозам бизнес-процессу в рамках стратегии разноуровневых предложений по восстановлению и противодействию информационным угрозам организации

Ключевые слова: модель, бизнес, процесс, организация, экономика.

Российские компании активно инвестируют в защиту от хакерских атак. В 2018 году инвестиции в информационную безопасность в IT-бюджетах увеличились до 22%. Средний IT- бюджет бизнеса в Российской Федерации составил $1,1 млн. В ближайшие три года произойдёт рост ещё на 18% из-за того, что инфраструктура информационных технологий в компаниях развивается, и им необходимы профессиональные знания по кибербезопасности, говорится в проведённом исследовании «Лаборатории Касперского». Финансовый ущерб российских компаний от утечек данных возрос за последние полгода. Для крупного бизнеса он примерно составил $246 тыс., на 2,5% больше, чем в прошлом году, говорится в исследовании «Лаборатории Касперского». Для среднего – вырос втрое – до $74 тыс. Ущерб, причиняемый кибератаками, становится все больше, шире и серьезнее и включает в себя финансовые и стратегические потери. Некоторые кибератаки, предположительно, являются частью интересов национальных или государственных кампаний. Кроме того, некоторые эгоистично действующие фирмы могут намеренно ограничивать свои инвестиции в кибербезопасность и полагаться на информацию, которую предоставят другие организации, чтобы защитить себя. Это может привести к недостаточным инвестициям в кибербезопасность, если все участники примут одну и ту же стратегию [4].

Практики бизнеса и его менеджмента выделяют две диаметральных формулировки задачи, которые определяют то, какая методология описания процессов наиболее приемлема и будет максимально эффективна – это, когда

постановка задачи звучит- «…для решения поставленных задач необходимо одним из этапов создать функциональную (процессную) модель компании, отображающую структуру, взаимосвязи и функции системы, а также потоки информации и материальных объектов, связывающих эти функции» [8].

Для целей обеспечения информационной безопасности такой модели ведения бизнес- процесса важно будет определить локализацию бюджетов для этапов производства и продажи продукции, услуг. Суммы возможных ущербов будет зависеть от мер какими будет обеспечена инфраструктура «движения информации» между отделами с позиции возможных кибератак конкурентов данной фирмы с целью остановить или нарушить весь бизнес-процесс, создать «временной ущерб» остановки бизнес-процесса.

Вторая модель бизнес-процесса по-другому описывает «движение информации» и звучит как – «…необходимы описания алгоритмов (сценариев) выполнения процессов в виде её участников. Прежде всего, определяются работники и причинно-следственные связи, временные последовательности выполнения ими хозяйственных действий, как упорядоченную комбинацию событий и функций работников». В этом случае упор делается на описание последовательностей действий, определение начальных и конечных событий, выявление участников, исполнителей, материальных и документальных потоков [3].

Для целей обеспечения информационной безопасности второй модели ведения бизнес-процесса важно будет определить локализацию информационных потоков между работниками организации, и задача кибермошенника будет состоять в том, чтобы максимально «усложнить» - «обнулить» информацию между этапами производства и продажи продукции, услуг с позиции внесения хаоса, дезориентирования работников фирмы, нарушения целостности информации, которая обсуживает бизнес-процесс.

Существующие подходы по описанию бизнес-процессов, как и существующее программное обеспечение, за редким исключением, специализированы и плохо подходят для решения тех задач, для которых они не были предназначены изначально [1]. Ниже на рисунке 1 представлено детальное описание бизнес-задачи по субъектам бизнес-процесса на примере условной коммерческой организации, в виде бизнес-задача А4.2 «Реализация проекта». Каким же образом, представленный на рисунке 1 бизнес-процесс, специалисту по информационной безопасности необходимо будет обезопасить сам бизнес-процесс.

Во-первых, необходимо использовать действующие на текущий момент времени в РФ стандарты информационной безопасности.

Во-вторых, необходимо классифицировать угрозы бизнес-процессу и разработать модернизированный вариант известной модели угроз по известному приказу ФСТЭК РФ от 11 февраля 2013 г. N 17, в котором защита персональных данных и рассматриваемый нами бизнес- процесс, имеет те-же особенности, что и при составлении модели угроз применительно к бизнес-процессу. К таковым особенностям можно отнести: зона вероятных угроз, вид

информационного актива, который будет подвержен угрозе, вид воздействующего фактора угрозы и показатели бизнес-процесса организации, которые будут подвержены угрозе [10].

Согласно данного стандарта организации всех типов и размеров накапливают, обрабатывают, сохраняют и передают информацию в различных формах, включая электронную, физическую и устную [6].

Ценность информации не только в документированных словах, числах и изображениях: знания, понятия, идеи и бренды – вот примеры нематериальных форм информации.

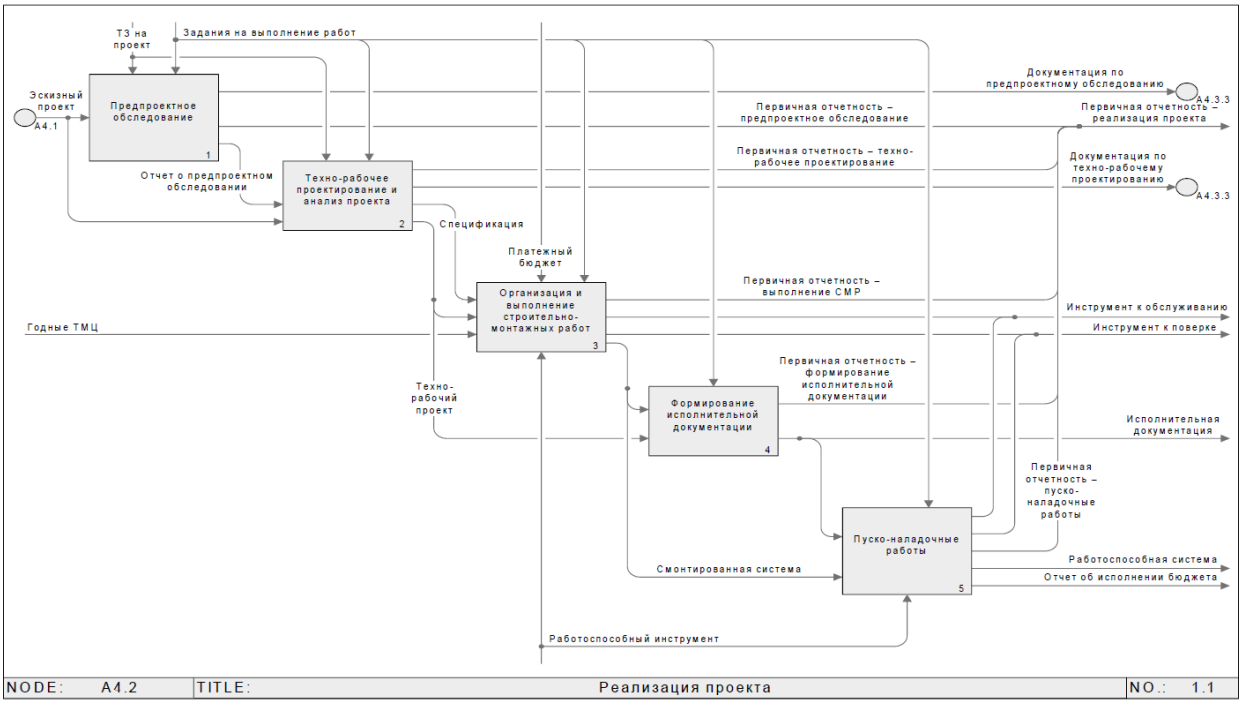

Рис. 1 – Бизнес-процесс для задачи А.4.2
«Реализация проекта по заказу клиента»

В мире, где все взаимосвязано, информация и соответствующие бизнес-процессы, системы обслуживающие бизнес-процесс, информационные сети которые объединяют все в единый процесс и персонал, функционально осуществляющий их эксплуатацию, обработку и защиту – все это информационные активы, которые, подобно другим важным деловым (наполненным ценностью) финансовым и материальным активам [9].

Рассмотрим перечисленные угрозы и сведем их в модернизированную модель угроз для бизнес-процесса коммерческой организации.

Но вначале на рисунке 2 отразим локализацию информационных угроз для коммерческой организации выполняющие задачу А4.2 с указанием зон рисков проникновения злоумышленника.

Особо-значимым звеном бизнес-процесса для каждой организации выделим блок-звено, известное как «расчетно-кассовое обслуживание» и его возможный «ущерб», как – время простоя получения аванса или итога дохода от выполнения бизнес-задачи А4.2.

С позиции информационных киберугроз, любой target вирус, проникший в системы компании по точкам входа, а именно любое оборудование компании может быть потенциально уязвимым, может вызвать как отказы в обслуживании кассовых систем, так и нелегитимный перевод средств на «лже-счета» злоумышленника.

В тоже время известный в бизнес-процессе любой организации этап как согласование дизайн-макета проекта заказчика и любой target вирус, проникший в системы компании по точкам входа, приведет к времени простоя для калькулирования и утверждения старта монтажных работ по данному клиентскому договору.

Также известный этап бизнес-процесса как «калькулирование» заказа клиента, после локальной target атаки на информационную систему компании, повлечет неисполнение договора на заказ, в виде времени простоя на этапах монтажа, установки оборудования, для калькулирования и утверждения старта монтажных работ.

Здесь не менее важна информационная безопасность от атаки на компании-посредники или на поставщиков, через внедрение в информационную систему организации «лже»-договоров в бизнес-процесс организации. Необходимо выделить также возможные вынужденные производственные простои от третьих лиц (электроснабжение, отсутствие комплектующих и прочее) при вводе в эксплуатацию заказа клиента, путем локальных DDoS-атак на IP-телефонии. Также вероятно будет отсутствие доступа к базе данных комплектующих, изменение ее содержимого или внезапный отказ обеспечения комплектующими, и как следствие задержка старта монтажа или ввода в эксплуатацию заказа [5].

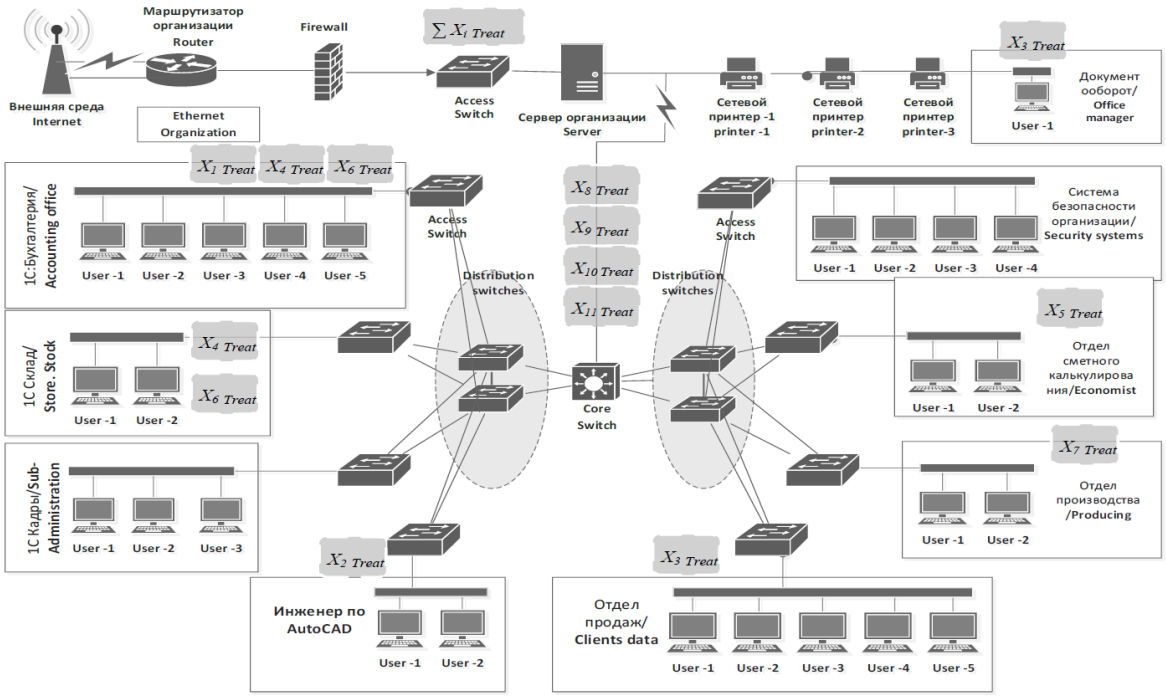

Рис. 2 – Зоны рисков информационной безопасности бизнес-задачи A4.2 (в составе бизнес-процесса)

Также широко-известными угрозами для бизнес-процесса организации являются - срыв поставки комплектующих для исполнения заказа. Упомянем также возможный технический отказ (сбой) установленного после монтажа оборудования заказа клиента (время демонтажа, последующие переделки и ожидание поставки новых комплектующих).

К наиболее вероятным угрозам можно отнести заражение всех информационных активов компании и уничтожение данных (включая все существующие проекты, документы, отчетности и прочие этапы, и ключевые факторы бизнес-процесса).

К наименее вероятным информационным угрозам, но вполне осуществимыми в условиях конкурентной борьбы организации за нишу рынка будет полное нарушение информационной целостности ПО или АО оборудования организации, по известному примеру Tailored Access Operations, с возможностью перехвата управления или уничтожения данных.

К совсем «нереальным», но все-таки учитываемым информационным угрозам надо отнести создание «клона заказчика» (или целевая атака на длительное время с последующим уничтожением компании).

Сведем представленные классификации информационных угроз и отразим данные факторы в модернизированной модели угроз в таблице 1.

Таблица 1 – Модернизированная модель угроз бизнес-процесса организации (по стандарту ISO/IEC 27001:2013 (E))

№ пп	Звено (отдел) бизнес-процесса организации	Вид возможной информационной угрозы для звена бизнес-процесса организации	Информационный актив организации, подвергаемый угрозе	Вид возможного ущерба	Вид угрозы	Показатель бизнес-процесса подвергаемый угрозе	Противодействие
1	2	3	4	5	6	7	8
1	Отдел бухгалтерского учета	Сбой или отсутствие расчетно-кассового обслуживания всей организации, в виде отказов в обслуживании кассовых систем, или также нелегитимный перевод средств на «лже»-счета злоумышленника или дополнительные расходы при покупке, настройки, обслуживании вышедшего из строя оборудования.	База данных учета операций бизнес-процесса 1С: Бухгалтерия	Время простоя получения аванса от заказчика или недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование отдела бухгалтерского учета которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Microsoft Windows Server 2016 Standard 64- bit Russian 1pk DSP OEI DVD 16 Core ~70000 руб.)
2	Отдел дизайна	Сбой в процессе согласования дизайн-макета проекта с заказчиком	База данных учета и хранения эскизов макет- дизайнов для заказчика Adope Photoshop	Время простоя получения аванса от заказчика или недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование отдела дизайна которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.

3	Отдел продаж, Офис-менеджер организации	Сбой в процессе исполнения клиентского договора, в виде времени простоя на этапах монтажа, установки оборудования, для калькулирования и утверждения старта монтажных работ; а также параллельные атаки на компании-посредники или на поставщиков, подмена договоров на лже-договоры.	База данных контрактов с клиентами и посредниками "Электронный документооборот"	Время простоя получения итогового дохода (выручки) от заказчика или недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование отдела монтажа которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.
4	Отдел бухгалтерского учета, Склад организации	Сбой в процессе доступа или отсутствие такого доступа к базе данных комплектующих, изменение ее содержимого или внезапный отказ обеспечения комплектующими (задержка старта монтажа или ввода в эксплуатацию.	База данных учета операций бизнес-процесса 1С: Склад	Время простоя общего времени монтажа и исполнения клиентского договора влекущее недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование 1С:Склад которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.
5	Отдел смет и мат-технического сопровождения	Сбой или отсутствие доступа к базе данных смет и комплектующих, изменение их содержимого или внезапный отказ обеспечения комплектующими (задержка старта монтажа или ввода в эксплуатацию);	База данных учета операций бизнес-процесса 1С: Сметы	Время простоя до подписания и начала старта исполнения клиентского договора влекущее недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование 1С:Склад которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз
6	Отдел бухгалтерского учета, Склад организации	Сбой или полный срыв поставки комплектующих для исполнения заказа по уже заключенным договорам с клиентами	База данных учета операций бизнес-процесса 1С: Склад	Время простоя при исполнении клиентского договора - влекущее недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование 1С:Склад которое потенциально уязвимо.	Затраты на создание информационного актива Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.
7	Произв одств енный отдел (монтаж, инженерия)	Сбой или технический отказ уже установленного по договору с клиентом смонтированного оборудования (время демонтажа, последующие переделки и ожидание поставки новых комплектующих);	Бизнес-процесс (производство работ, услуг по основной деятельности организации)	Время простоя общего времени по окончании монтажа по клиентскому договору влекущее недополучение сумм дохода от бизнес-процесса	Любой target вирус проникший в систему Network организации - например точки входа в любое оборудование 1С:Склад которое потенциально уязвимо.	Затраты отдела монтажа организации Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.
8	Все отделы организации	Сбой бизнес- процесса или вынужденные производственные простои от третьих лиц (э/снабжение, отсутствие комплектующих и прочее) при вводе в эксплуатацию системы инф безопасности; (DDoS-атаки на IP-телефонию, противодействие - контроль доступа и политика аудита)	Бизнес-процесс (производство работ, услуг по основной деятельности организации)	Время простоя при исполнении клиентского договора - влекущее недополучение сумм дохода от бизнес-процесса	Любая DDoS-атака на систему Network организации - любое оборудование всей организации	Затраты организации Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.
9	Все отделы организации	Уничтожение информационного	Бизнес-процесс (производство	Потеря информационного	Любая DDoS-атака или вирус -	Затраты организации	Установка контроля

		актива путем заражения всех информационных активов компании и уничтожение данных (включая все существующие проекты, документы, отчетности и прочие факторы бизнес- процесса.	работ, услуг по основной деятельности организации)	актива организации	атака на периметр сети - Network организации	Доход организации	доступа. Адекватная политика безопасности. Создание модели угроз.
10	Все отделы организации	Сбой, отказ в доступе или полное нарушение информационной целостности ПО или АО оборудования (как пример Tailored Access Operations) с возможностью перехвата управления или уничтожения данных	Бизнес-процесс (производство работ, услуг по основной деятельности организации)	Время простоя при исполнении клиентского договора - влекущее недополучение сумм дохода от бизнес-процесса	Любая DDoS-атака на систему Network организации - любое оборудование всей организации	Затраты организации Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.
11	Все отделы организации	Потеря времени - "холостой" бизнес-процесс от создания злоумышленниками клона заказчика-клиента (целевая атака на длительное время с последующим уничтожением компании)	Бизнес-процесс (производство работ, услуг по основной деятельности организации)	Время "холостого" обслуживания при исполнении "лже"-клиентского договора - влекущее недополучение сумм дохода от бизнес-процесса	Любая DDoS-атака на систему Network организации - оборудование всей организации	Затраты организации Доход организации	Установка контроля доступа. Адекватная политика безопасности. Создание модели угроз.

Информационные активы организации подвержены как реднамеренным, так и случайным угрозам, при этом связанные с ними процессы, системы, сети и люди имеют присущие им уязвимости [7].

Изменения бизнес-процессов и систем или другие внешние изменения (такие как новые законы и регламенты) могут создать новые риски для информационной безопасности. Поэтому, учитывая множество способов, которыми угрозы киберпреступников, используя уязвимости «этапов» и «блоков» бизнес-процесса, могут нанести вред организации, можно уверенно утверждать, что риски информационной безопасности всегда присутствуют.

Система менеджмента информационной безопасности (сокращенно СМИБ), как это определено в ISO/IEC 27001 [2], дает целостное, согласованное представление о рисках организации в сфере информационной безопасности в целях осуществления всестороннего комплекса мер по обеспечению информационной безопасности в рамках целостной системы менеджмента. Многие информационные системы были разработаны без учета требований к безопасности в контексте ISO/IEC 27001 и этого стандарта. Безопасность, обеспечиваемая только техническими средствами, носит ограниченный характер и должна быть дополнена соответствующим менеджментом и процедурами.

Определение, какие средства использовать в конкретном случае, требует тщательного планирования и внимания к деталям. Для успешного функционирования СМИБ требуется ее поддержка всеми сотрудниками организации. Это может также потребовать участия акционеров, поставщиков или других внешних сторон. Также могут потребоваться советы привлекаемых извне специалистов.

Таким образом, мы можем приступить к разработке адекватной стратегии информационной безопасности в рамках предложенной модели угроз для объекта исследования.

Список литературы

1. Баранников А.Л. Развитие интеллектуального капитала и инновационных компетенций / А.Л. Баранников, С.П. Иванова, О.В. Барбашина, О.В. Грибкова, Д.К. Балаханова // В сборнике: Актуальные вопросы обеспечения образовательной и научной деятельности в университете сборник статей. Москва, 2016. С. 5-8.
2. Бойченко О.В. Решение проблем сетевой безопасности на уровне DDoS, труды IV международная научно-практическая конференции, Симферополь-Гурзуф, 5-17 февраля 2018 г. С. 4-7.
3. Дубов Д.А., Колпаков В.Ф Выбор подходящей модели для моделирования экономических процессов / Д.А. Дубов, В.Ф. Колпаков//Экономика и предпринимательство. -2017.-№ 4-2 (81-2).-С.132-135.
4. Иванова С.П. Принципы построения и особенности организационно-экономического проектирования интегрированных структур различных типов / С.П. Иванова // Устойчивое развитие российской экономики: материалы III Международной научно-практической конференции. - 2016. - С. 48-52.
5. Колпаков В.Ф. Моделирование динамических процессов в экономике/В.Ф. Колпаков//Финансовая аналитика: проблемы и решения. 2014. № 3. С. 31-36.
6. Мясоедов А.И. Инновационные технологии в управлении персоналом / А.И. Мясоедов // В сборнике: Инновационная экономика и менеджмент: Методы и технологии Сборник материалов II Международной научно-практической конференции. Под ред. О.А. Косорукова, В.В. Печковской, С.А. Красильникова. 2018. С. 222-224.
7. Мясоедов А. И. Устоявшиеся подходы к организации информационного пространства интернет-СМИ / А.И. Мясоедов // Скиф. Вопросы студенческой науки. 2017. № 15 (15). С. 219-223.
8. Пряжникова Е.Ю. Психология труда: теория и практика: учебник для бакалавров / Е. Ю. Пряжникова. -М.: Издательство Юрайт, 2019. -452 с.
9. Радостева М.В. К вопросу о производительности труда / М.В. Радостева // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. - 2018.-Т.45.-№2.- С.268-272.
10. Радостева М.В. Производительность труда: основные тенденции и ключевые факторы развития на современном этапе /М.В. Радостева // Экономика и менеджмент систем управления. 2018. Т. 29. № 3-1. С. 162-172.