ISSN 2587-5922

ТЕОРИЯ И ПРАКТИКА ПРОЕКТНОГО ОБРАЗОВАНИЯ

№ 2 (10) / 2019

Журнал научных публикаций

Учредитель: ООО «ФАГОТ-ИНЖИНИРИНГ», ЦНИИ института русского жестового языка

E-mail: info@journaltppo.ru

Сайт: http://journaltppo.ru/

Почтовый адрес: 107241, г. Москва, Черницынский проезд, д. 3

Шеф-редактор: Олейник Андрей Владимирович

Председатель редакционного совета журнала: Харламенков Алексей Евгеньевич

Главный редактор: Бритвина Валентина Валентиновна

Технический редактор и корректор: Муханова Анна Александровна

Верстка: Муханов Сергей Александрович

http://journaltppo.ru/

ISSN 2587-5922

ТЕОРИЯ И ПРАКТИКА ПРОЕКТНОГО ОБРАЗОВАНИЯ

Журнал научных публикаций

РЕДАКЦИОННЫЙ СОВЕТ ЖУРНАЛА

учной работе РГУ нефти и газа (НИУ) им. И.М. Губкина, Член Совета Директоров (ВОА) Европейской федерации коррозионистов (Великобритания).

Молчанов Игорь Николаевич, доктор экономических наук, профессор, профессор кафедры политической экономии Экономического факультета Московского государственного университета имени М.В. Ломоносова, профессор, Департамента общественных финансов Финансового университета при Правительстве Российской Федерации.

Нижников Александр Иванович, доктор педагогических наук, кандидат физико-математических наук, профессор, Заслуженный работник высшей школы Российской Федерации, Почётный работник высшего профессионального образования Российской Федерации, заведующий кафедрой технологических и информационных систем МИГУ

Олейник Андрей Владимирович, доктор технических наук, профессор, лауреат премии Правительства Российской Федерации в области науки и техники, лауреат премии Правительства Российской Федерации в области образования, заведующий кафедрой «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН».

Разумова Татьяна Олеговна, доктор экономических наук, профессор, заведующий кафедрой экономики труда и персонала Экономического факультета МГУ имени М.В. Ломоносова.

Смирнова Вероника Ремовна, доктор экономических наук, профессор, проректор по научной работе Российской государственной академии интеллектуальной собственности.

Устинова Лилия Николаевна, доктор экономических наук, профессор кафедры «Управление инновациями и коммерческое использование интеллектуальной собственности» Российской государственной академии интеллектуальной собственности.

Червяков Леонид Михайлович, доктор технических наук, профессор, лауреат премии Правительства в области образования, Лауреат премии Правительства в области науки и техники, почетный работник высшего профессионального образования Российской Федерации, академик Академии проблем качества.

Филиппович Андрей Юрьевич, декан факультета Информационных технологий, профессор кафедры «Инфокогнитивные технологии» Московского политехнического университета, кандидат технических наук. Эксперт Минобрнауки России, АПКИТ, СПК-ИКТ, ФУМО в сфере ИТ, World Skills Россия.

Щербак Евгений Николаевич, доктор юридических наук, профессор Российской государственной академии интеллектуальной собственности, Полковник ВВС, военный летчик-истребитель 1-го класса, Почётный работник высшего профессионального образования Российской Федерации, Академик РАЕН.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Шеф- редактор

Олейник Андрей Владимирович.

Научный редактор

Бондарь Валентин Степанович.

Главный редактор

Бритвина Валентина Валентиновна.

Заместитель главного редактора

Чаттаев Азамат Русланович.

Муханов Сергей Александрович.

Ответственный редактор раздела «Естественно-научная проектно-исследовательская деятельность в учебном заведение»

Бычкова Наталья Александровна.

Ответственный редактор раздела «Правовое обеспечение в сфере науки, технологий и образования»

Сушкова Ольга Викторовна.

Ответственный редактор раздела «Проектирование и прогнозирование в социально-экономической сфере»

Пятаева Ольга Алексеевна.

жмента и экономики спорта имени В. В. Кузина Российского государственного университета физической культуры, спорта, молодежи и туризма «ГЦОЛИФК».

Загребельная Наталья Станиславовна, декан факультета прикладной экономики и коммерции, кандидат экономических наук, доцент кафедры менеджмента, маркетинга и внешнеэкономической деятельности им. И.Н. Герчиковой Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации.

Змазнева Олеся Анатольевна, кандидат философских наук доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета.

Канапьянов Серик Хабдульмуталяпович, полковник, кандидат педагогических наук, методист Учебно-методического управления Национального университета обороны имени Первого Президента Республики Казахстан-Елбасы.

Конюхова Галина Павловна, кандидат педагогических наук, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН».

Лхагвасурэн Гундэгмаа, PhD, проректор Национального Института Физической культуры Монголии.

Микола Седак, преподаватель права, доцент Университета Коменского в Братиславе, Словакия.

Моргунов Юрий Алексеевич, кандидат технических наук, доцент, декан факультета базовых компетенций Московского политехнического университета.

Муханов Сергей Александрович, кандидат педагогических наук, доцент кафедры «Математика» Московского политехнического университета.

Пятаева Ольга Алексеевна, кандидат экономических наук, доцент, заведующий кафедрой «Международные экономические и финансовые отношения» Российской государственной академии интеллектуальной собственности (РГАИС).

Скареднова-Вайс Екатерина Алексеевна, председатель Подкомитета Московской торгово-промышленной палаты по проблемам ведения бизнеса.

Сушкова Ольга Викторовна, кандидат юридических наук, доцент, доцент кафедры Предпринимательского и корпоративного права Московского государственного юридического университета им. О.Е. Кутафина (МГЮА), доцент кафедры предпринимательского, трудового и корпоративного права Юридического факультета РАНХиГС.

Филиппович Юрий Николаевич, кандидат технических наук, профессор кафедры «Инфокогнитивные технологии» Московского политехнического университета.

Хмыз Алексей Иванович, кандидат юридических наук, подполковник полиции, старший преподаватель кафедры «Оружиеведения и трасологии учебно-научного комплекса судебной экспертизы» Московского университета МВД России имени В.Я. Кикотя.

Чаттаева Виолетта Раисовна, кандидат юридических наук, старший преподаватель кафедры «Управления и гражданское право» Института Деловой Карьеры.

Чикунов Иван Михайлович, кандидат технических наук, заведующий кафедрой «Инфокогнитивные технологии» Московского политехнического университета.

Чаттаев Азамат Русланович, кандидат юридических наук, доцент кафедры гражданско-правовых дисциплин АНО ВУ «Открытый Гуманитарно-Экономический Университет».

Щербак Анна, кандидат юридических наук, сотрудник Bureauvan Dijk, a Moody's Analytics Company, Женева, Швейцария.

УЧРЕДИТЕЛИ:

Харламенков Алексей Евгеньевич, директор центрального научно-исследовательского института русского жестового языка. Эксперт НИУ ВШЭ, эксперт по информационным технологиям в области электронных документов, старший преподаватель кафедры «Инфокогнитивные технологии» Московского политехнического университета.

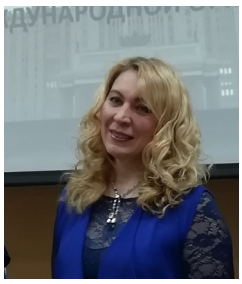
Седенков Сергей Евгеньевич, преподаватель кафедры «Туризма и гостиничного дела» Российского государственного университета физической культуры, спорта, молодежи и туризма.

СОДЕРЖАНИЕ

РАЗДЕЛ I. ЕСТЕСТВЕННО-НАУЧНАЯ ПРОЕКТНО-ИССЛЕДОВАТЕЛЬСКАЯ ДЕЯТЕЛЬНОСТЬ В ВУЗЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ: ВНЕДРЕНИЕ СИСТЕМЫ АНАЛИЗА ДАННЫХ В ВУЗ

Кривоногов Антон Алексеевич
техник по защите информации ООО Русское Техническое Общество



Бритвина Валентина Валентиновна
кандидат педагогических наук, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН», доцент кафедры Инфокогнитивных технологий Московского политехнического университета

Аннотация: *В статье описана возможность внедрения системы анализа данных, предназначенная для улучшения и расширения функционала управления вузом и обеспечения его информационной безопасности. Рассмотрены состав и особенности эксплуатации системы безопасности вуза после внедрения системы анализа данных.*

Ключевые слова: *информационная безопасность, система анализа данных, цифровые технологии, инциденты, вуз.*

Abstract: *The article describes the possibility of using a data analysis system designed to improve and expand the functionality of security management. Considered the composition and features of the operation of the security system.*

Keywords: *information security, data analysis system, digital technologies, incidents, university.*

Введение. В последние годы в сфере образования наблюдается тенденция внедрения цифровых технологий, которые дают новые инструменты для развития университетов и других образовательных учреждений во всем мире. Почти каждый вуз сталкивается в той или иной мере с необходимостью детального анализа данных, которые накапливаются в процессе деятельности учебного учреждения. Но вручную, в период развития цифровых технологий, сбор и анализ данных осуществлять нецелесообразно. Поэтому в РФ происходит повсеместное внедрение системы анализа данных в образовательный процесс. [3]

Цель исследования - изучить применение системы анализа данных в вузе.

Задачи исследования.

- Проанализировать вузы РФ на внедрение системы анализа данных в учебный процесс;
- Рассмотреть основные возможности использования системы анализа данных в масштабах вуза;
- Сравнить программные комплексы и выбрать оптимальную систему для внедрения в вуз.

Под системой анализа данных следует понимать специализированный программный комплекс, который будет получать и обрабатывать всю поступающую информацию в информационном пространстве вуза. Применение системы анализа деятельности вуза позволит администрации получать оперативно сведения обо всех событиях (инцидентах) происходящих за данный период времени и предпринимать соответствующие решения.

Как видно на рисунке 1, всего в 55% случаев в учебных заведениях используется электронный документооборот, вследствие этого могут возникать ситуации, когда специалистам учебного отдела необходимо установить какую-либо информацию об учебном процессе (список студентов-отличников, список студентов с задолженностями и посещения занятий), им придется выполнить огромную работу, а именно: отобрать из ведомостей итоги зачетов, экзаменов, выписать из журналов посещаемости сведения о пропусках занятий. Также можно заметить, что в 15% случаев в вузах происходит внедрение цифровых

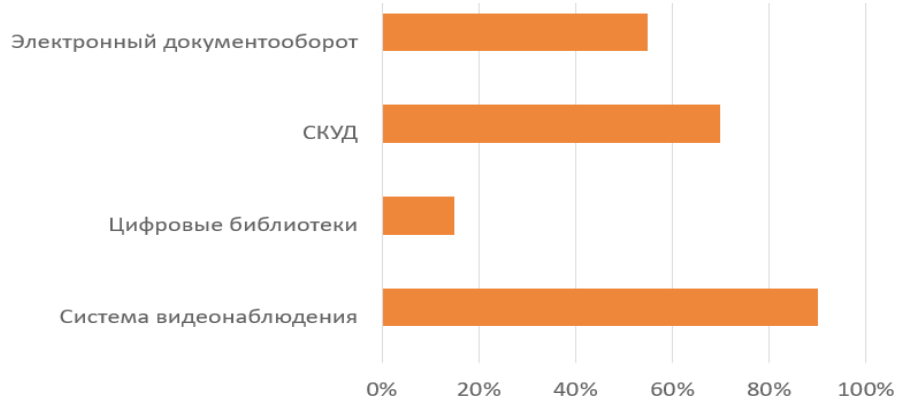


Рисунок 1. Анализ внедрения технологий анализа данных в вузах

библиотек, хотя эта технология является необходимой для обеспечения более высокого уровня комфорта для студентов и преподавателей, а также позитивно влияет на имидж вуза. Нельзя не отметить, что во многих вузах (в 90% случаев) используется система видеонаблюдения, что дает нам контроль над учебным заведением и предотвращает от возникновения большого числа инцидентов. В 70 % случаев учебные заведения используют систему контроля управлением доступом (СКУД), которая позволяет осуществлять контроль доступа на заданную территорию, а также может использоваться совместно с системой видеонаблюдения (для совмещения архивов событий систем) и с системой пожарной сигнализации (для получения информации о состоянии пожарных извещателей, автоматического разблокирования эвакуационных выходов и закрывания противопожарных дверей в случае пожарной тревоги).

Из рисунка 1 следует, что все эти технологии очень полезны и их необходимо повсеместно внедрять во все учебные заведения, чтобы предотвращать все неудобства и инциденты, а также для того, чтобы в ближайшем будущем поднять учебный процесс на новый, более высокий уровень. Для всего этого необходимо использовать технологию анализа данных.

Возможности, полученные пользователями при внедрении системы анализа данных, зависят от её масштаба. Спектр её возможностей зависит от конкретных алгоритмов функционирования. На данный момент не во всех вузах реализована данная технология в полном объеме, в результате чего становится невозможным принятие быстрых решений при возникновении инцидентов. [2]

Основные возможности использования системы анализа данных в масштабах вуза представлены на рисунке 2.

Рассмотрев возможности системы анализа данных, необходимо исследовать ее внедрение в пространство вуза, а именно, понять эффективность данной системы, способна ли она помочь снизить количество инцидентов в информационном пространстве вуза. Сравнительный анализ возникновения инцидентов до и после внедрения системы анализа данных показан на рисунке 3.

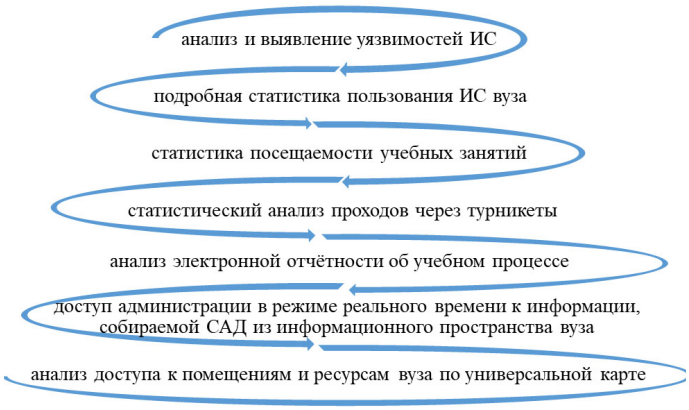


Рисунок 2. Основные возможности использования системы анализа данных

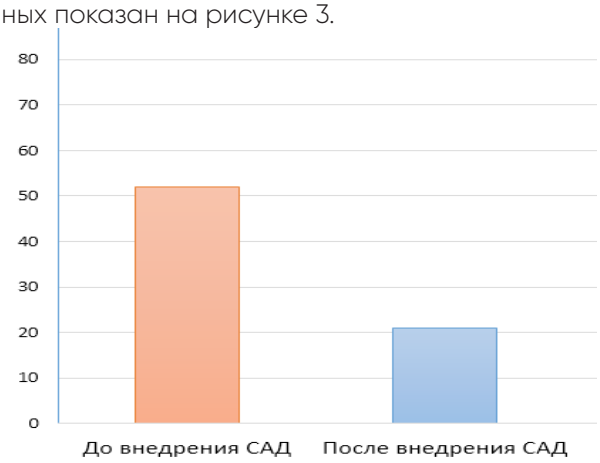


Рисунок 3. Статистика возникновения инцидентов

Исходя из исследования, внедрение системы анализа данных в информационное пространство вуза повлияет на снижение количества инцидентов, а именно, вероятность возникновения снизится в среднем на 50 %.

На рисунке 4 представлены готовые программные решения для анализа данных.

Как видно, на рисунке 4 представлены следующие системы анализа данных. Необходимо проанализировать готовые программное решения для анализа данных и выбрать оптимальный вариант для внедрения в вуз.

Начнем обзор программных решений с уни-

Рисунок 4. Готовые программные решения для анализа данных

версальной интегрированной системы STATISTICA, которая была разработана компанией StatSoft. Данная система предназначена для статистического анализа и визуализации данных, а также для управления базами данных и разработки пользовательских приложений. Продукт реализует самые современные компьютерные и математические методы анализа данных, а именно: анализ многомерных таблиц, методы описательной статистики, кластерный анализ, нелинейная регрессия и другие. Эта система позволяет обмениваться данными с наиболее популярными СУБД, а также с удаленными базами данных. Кроме пакета STATISTICA компанией StatSoft были разработаны следующие продукты, который используют современные технологии Data Mining (интеллектуальный анализ данных): STATISTICA Data Miner, STATISTICA Neural Networks и STATISTICA Power Analysis. Цены на эти продукты довольно умеренные для программ такого класса. В частности, русскоязычная однопользовательская версия программы STATISTICA 6.0 стоит около 150000 рублей. Однако, для учебных учреждений ее можно приобрести всего лишь за 60000 рублей. Но несмотря на большое количество реализованных методов анализа и удобный интерфейс, программы пакета STATISTICA довольно сложны в использовании, поскольку требуют от пользователя как определенных математических знаний, так и знаний в области анализа данных, что может затруднить их использование сотрудниками вуза. [1, 2]

Перейдем к рассмотрению следующего программного решения для анализа данных. Oracle Data Mining представляет собой инструмент анализа данных, который поставляется вместе с СУБД Oracle Enterprise Edition. Этот инструмент представляет собой отдельный модуль. Он поддерживает все этапы технологии извлечения знаний, включая постановку задачи, подготовку данных, построение модели, анализ и тестирование результатов. Oracle Data Mining реализует следующие методы анализа данных: поиск ассоциаций, кластеризация, выделение признаков, поиск существенных атрибутов. Преимущество перечисленных алгоритмов состоит в том, что они работают непосредственно с реляционными базами данных и не требуют выгрузки данных в файлы специальных форматов. Стоимость данного инструмента составляет около 20000 рублей. Указанная цена приведена для одной лицензии (т.е. одновременно может поддерживаться только одно подключение). Сама СУБД Oracle стоит более 350000 рублей. Препятствием к использованию данного инструмента является то, что корпоративная база данных вуза управляется СУБД MS SQL Server, и покупать еще одну серверную СУБД будет, как минимум, дорого и нецелесообразно. [1]

Наконец, рассмотрим еще один программный продукт PolyAnalyst, который был разработан российской компанией Мегакомпьютер Интеллидженс и который предназначен для анализа числовых и текстовых данных. Основное назначение этого программного продукта – обнаружение полезных знаний, необходимых для принятия решений в сфере образования, в бизнесе и других сферах человеческой деятельности. PolyAnalyst является клиент-серверным приложением, где модули анализа выделены в серверную часть PolyAnalyst Knowledge Server, а инструментарий пользователя – в клиентскую программу PolyAnalyst Workspace. Продукт включает в себя следующие классы алгоритмов анализа: моделирование, прогнозирование, кластеризация, классификация, текстовый анализ. PolyAnalyst поддерживает связь с базами данных через интерфейсы ADO и OLE DB, имеет богатый набор инструментов для графического представления результатов исследований. Цена на полный пакет программ, который входит в PolyAnalist, составляет около 350000 рублей. Цена на минимальный набор модулей системы анализа составит около 60000 рублей. [1, 3]

Сопоставив варианты готовых программных решений, целесообразно будет остановиться на выборе последнего инструмента анализа данных, а именно, PolyAnalist, т.к. за адекватную стоимость будет получено достаточно инструментов для анализа данных. Плюсом также является то, что данный инструмент разработан российской компанией. Единственное, что может потребоваться для эффективной работоспособности данной системы – это обучение сотрудников вуза для дальнейшей работы с данным инструментом.

Вывод. Проанализировав внедрение системы анализа данных в вузах РФ можно сделать вывод, что не во всех учебных заведениях в полной мере реализована данная технология, а, следовательно, необходимо обеспечить повсеместное внедрение системы анализа данных в учебные заведения. Рассмотрев основные преимущества системы анализа в масштабах вуза, следует понимать, что в наше время внедрение системы анализа – это необходимый шаг для всех учебных заведений. Также сравнив возможные системы анализа, было принято решение, что целесообразно внедрить программный продукт PolyAnalist в информационное пространство вуза для обеспечения должного уровня контроля и уменьшения возникновения инцидентов. Использование данной системы приведет к тому, что итоги анализа данных впоследствии смогут использоваться для принятия сложных управленческих решений вуза, а также для решения различных вопросов в таких областях, как учебной, административной, финансовой и других.

Список литературы

1. Барсегян А., Куприянов М., Степаненко В., Холод И. Методы и модели анализа данных: OLAP и Data Mining. Учебное пособие – СПб.: БХВ-Петербург, 2004.
2. Кривенко М. П., Уфимцев М. В. Методы анализа данных. — Изд-во Академии ФСБ Москва, 2002. — 475 с.
3. Миркин Б.Г. Введение в анализ данных: учебник и практикум для бакалавриата и магистратуры. — М.: Юрайт, 2014.

РАЗДЕЛ II. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ В СФЕРЕ НАУКИ, ТЕХНОЛОГИЙ И ОБРАЗОВАНИЯ

АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ ПЕРСПЕКТИВНОЙ ТЕХНОЛОГИИ НЕЙРОКОМПЬЮТЕРНОГО ИНТЕРФЕЙСА

Баев Илья Андреевич
АО «БИФИТ»
DevOps инженер-программист

Береснева Яна Владиславовна
старший преподаватель кафедры «Инфокогнитивные технологии» Московского политехнического университета, старший преподаватель кафедры специальных вычислительных комплексов, программного и информационного обеспечения автоматизированных систем управления и робототехнических комплексов Военной академии ракетных войск стратегического назначения имени Петра Великого.

Аннотация: *в статье описаны субъективные представления о потенциальных угрозах, положительном эффекте от развития и повсеместного проникновения технологии доступных двусторонних нейрокомпьютерных интерфейсов, способных транслировать визуальные образы в сознание, неотличные от реальных, подобно тому как это происходит во сне.*

Ключевые слова: *нейрокомпьютерный интерфейс, нейроинтерфейс, технологии, будущее, угрозы.*

Abstract: *the article describes the subjective perceptions of potential threats, the positive effect of the development and widespread penetration of technology available bilateral neurocomputer interfaces that can translate visual images into consciousness, indistinguishable from real, just as it happens in a dream.*

Keywords: *brain-computer interface, neural interface, technology, future, threats.*

Введение: Анализ потенциальных угроз нейрокомпьютерного интерфейса (далее – нейроинтерфейс) не является актуальной темой "сегодня", но будет таковой в следующем десятилетии. Причиной этому является низкая скорость прогресса в этой области в сравнении с актуальной сейчас областью искусственного интеллекта. Как и большая часть других технологий, массовое распространение и влияние нейроинтерфейс может получить после появления интереса со стороны сферы развлечений, как одной из самых широких и больших по объему средств сфер[4].

Цель исследования: изучить потенциальные угрозы перспективной технологии нейроинтерфейса.

Задачи исследования:

- Проанализировать потенциальные угрозы нейроинтерфесов;
- Рассмотреть применение и пользу нейроинтерфесов.

Нейроинтерфейс представляет собой мост между некой вычислительной техникой и мозгом человека. Может быть, как односторонним (в любом из

направлений), так и двусторонним.

В настоящее время ведется активная разработка технологий, которые можно использовать в медицине, в частности для создания мысленного интерфейса, который позволит людям с разного рода заболеваниями или травмами комфортно чувствовать себя в бытовом плане, за счет применения разработок роботизации, управляемых через нейроинтерфейс. В упрощенном виде взаимодействие человека и компьютера можно представить, как фокусировку на различного рода сигналах, которые через специализированное программное обеспечение считывается и преобразуется в команды для иных устройств. Известны попытки трансляции визуальных примитивов в мозг человека[2].

В текущем виде технологию нейроинтерфейса нельзя назвать опасной из-за ее слабого влияния на сознание человека. Мы рассмотрим перспективные нейроинтерфейсы, при которых будет достигнут уровень трансляции сигналов в мозг человека, не отличных от реального мироощущения. То есть, когда будет возможность подключиться к нейроинтерфейсу и перешагнуть границы нашего мира с его ограничениями. Ведь наше тело ограничено законами нашего мира, а наше сознание нашим воображением. Потенциальные угрозы нейроинтерфейсов представлены на рисунке 1.

Рисунок 1. Потенциальные угрозы нейроинтерфейсов

В качестве первого примера рассмотрим технологию, показанную в художественном фильме сестер (в прошлом братьев) Вачовски – "Матрица". В фильме большая часть людей живет с симуляции, а в реальном мире находятся в капсулах, поддерживающих их жизнеспособность и подключающих к симуляции через нейроинтерфейс (соединением напрямую с мозгом при помощи сигнального кабеля). Люди в симуляции не представляют о том, что в ней находятся и считают свою жизнь нормальной, проходящей в реальном мире. Это первая из потенциальных угроз развитой технологии нейроинтерфейса: люди, подключенные к виртуальному миру, могут не замечать разницы между мирами и в конечном итоге утратить связь с реальностью. Вместе с этим, человеку можно внедрить любую идею, которую станет считать естественной и действительной[3].

Следующий пример нейроинтерфейса возьмем из цикла произведений «ソードアート・オンライン" (яп.: со:до а:то онрайн) за авторством Рэки Кавахара и других. По сюжету произведения, игроки революционной игры, доступ к которой осуществлялся через нейроинтерфейс, были заточены в игре ее создателем с целью проведения социального эксперимента. В отличии от первого примера, здесь пользователи осознавали, что находятся в другом мире. Если в "Матрице" герои произведения занимались освобождением разумов людей от системы, то в «ソードアート・オンライン" это было невозможно из-за волнового воздействия устройства на мозг, в случае отключения которого, мозгу пользователя наносился невосполнимый ущерб, несопоставимый с жизнью. Это следующая из потенциальных угроз: вероятность быть насильно заточенным в мире, транслируемым через нейроинтерфейс. Осознание безысходности от невозможности вернуться в реальный мир без вреда для жизни и от осознания мира вокруг себя как нереального может свести с ума.

Последний примером будет художественное произведение "Ready Player One" Эрнеста Клайна. В нем не описан нейроинтерфейс, однако описан бедный мир, жители которого спасаются в мире виртуальном, где нет ограничений, нет бедности. В этом кроется следующая угроза: реальный мир может быть заброшен людьми, в пользу мира виртуального. Впоследствии это может привести к развалу человеческой цивилизации.

Рисунок 2. Варианты использования нейроинтерфейсов

Использование технологии в области медицины является одним из очевидных направлений применения технологии (Рисунок 2). Люди с проблемами опорно-двигательного аппарата, в перспективе смогут управлять роботизированными протезами мысленными сигналами также, как если бы это были естественные здоровые конечности. Людей с тяжелыми травмами можно помещать в особую систему, подобно тому, как сейчас используется медикаментозная кома, например, встретится с родственниками[1].

Для сферы развлечений, взаимодействие напря-

мую с мозгом открывает бесконечные границы. Симуляция абсолютно любых ситуаций, выходящих за рамки возможного в реальном мире, поднимет уровень от интерактивных развлечений на запредельно высокий уровень.

Рисунок 3. Схема взаимодействия угроз и пользы

Вывод. Как и у любой другой технологии (ядерные технологии, искусственный интеллект, порох, и т.д.), технология нейроинтерфейса привнесет как пользу, так и своеобразную угрозу, и вред (Рисунок 3). С развитием технологии, область пользы будет все шире сходится с областью потенциальных угроз: будут расти возможности – будут расти и потенциальные пути их пагубного использования.

Можно сделать вывод, что технология нейрокомпьютерных интерфейсов не является опасной, как и подавляющее большинство развивающихся технологий.

Список литературы

1. Бехтерева Н. П., Нагорнова Ж. В. Динамика когерентности ЭЭГ при выполнении заданий на невербальную (образную) креативность // Физиология человека, 2007, т. 33, № 5, с. 5-11.
2. Иваницкий Г.А. Николаев А.Р., Иваницкий А. М. Использование искусственных нейросетей для распознавания типа мыслительных операций по ЭЭГ // Авиакосмическая и экологическая медицина, 1997, т. 31, с. 23-28.
3. Савельева-Новосёлова Н.А., Савельев А.В. Принципы офтальмонейрокибернетики // В сборнике "Искусственный интеллект. Интеллектуальные системы", Донецк-Таганрог-Минск, 2009, с. 117-120.
4. Петрунин Ю. Ю., Рязанов М.А., Савельев А. В. Философия искусственного интеллекта в концепциях нейронаук. (Научная монография), М.: МАКС Пресс, 2010, ISBN 978-5-317-03251-7.

ПРИМЕР РЕАЛИЗАЦИИ ИННОВАЦИОННЫХ РАЗРАБОТОК НА ОСНОВЕ ТЕСНОГО ВЗАИМОДЕЙСТВИЯ СТРУКТУР ИННО-ВАЦИОННОГО КЛАСТЕРА «ЮЖНОЕ СОЗВЕЗДИЕ»

Евсеев Олег Анатольевич
Российский сельскохозяйственный банк

Аннотация: *Статья посвящена вопросам функционирования пилотного инновационного кластера. Мировой опыт показывает, что наиболее удачной организационной формой для развития и продвижения инноваций служат инновационные кластеры.*

На примере инновационного кластера «Южное созвездие» рассматривается схема взаимодействия и кооперационные связи как между участниками внутри кластера, так и взаимодействие с внешней средой, описываются основные проекты и проблемы в деятельности кластера. Также рассматривается возможность встраивания в глобальную систему инновационных кластеров.

Ключевые слова: *инновационные кластеры, управление, примеры взаимодействия, факторы развития кластерных структур*

Abstract: *The article is devoted to the functioning of the pilot innovation cluster. World experience shows that innovative clusters are the most successful organizational form for the development and promotion of innovations.*

On the example of the Southern Constellation innovation cluster, the interaction scheme and cooperation links between the participants within the cluster and the interaction with the external environment are considered, the main projects and problems in the cluster's activities are described. The possibility of inte-grating into the global system of innovation clusters is also being considered.

Keywords: *innovation clusters, management, examples of interaction, factors of development of cluster structures*

Введение

На современном этапе общественной жизни именно инновации становятся основной движущей силой развития мировой экономики. Благодаря инновациям общество переходит на новую, более высокую ступень развития. Таким образом, государство, которое стремится к экономическому росту, должно, в первую очередь, уделять внимание развитию инноваций.

Целью данной статьи является показать примеры реализации инновационных разработок на примере инновационного кластера «Южное созвездие». Задачи, которые поставил автор – выделить факторы в пользу кластерного развития инноваций, дать краткую характеристику особенностям инновационных кластеров в России, а также описать структуру управления и внутреннюю структуру инновационного кластера «Южное созвездие», показать примеры инновационных разработок данного кластера, а также определить проблемы дальнейшего развития кластера «Южное созвездие».

Исследование выполнено на основе аналитических материалов трудов ученых, специалистов ВШЭ, материалов конференций и докладов ведущих специалистов, руководителей кластерных структур[2].

Объект исследования: пилотные инновационные кластеры

Предмет исследования: продвижение инноваций в кластерах, факторы, влияющие на результативность кластеров

Согласно определению родоначальника теории кластеров Майкла Портера, кластер - это группа географически соседствующих взаимосвязанных компаний и связанных с ними организаций, действующих в определенной сфере и взаимодополняющих друг друга. При этом благодаря синергетическому эффекту значительно усиливаются конкурентные преимущества отдельных участников кластера и кластера в целом [1]. Можно выделить следующие факторы в пользу именно кластерного развития инноваций:

- кластеры способствуют повышению эффективности деятельности мелких и средних компаний за счет доступа к единой научной и производственной инфраструктуре;
- внутри кластера проявляется эффект экономии на масштабах за счет разделения труда, специализации и снижения транзакционных издержек;
- появляется возможность свободного обмена информацией;
- благодаря объединению усилий компании способны решать задачи, которые не под силу решить им по отдельности;
- регионы повышают свою привлекательность для бизнеса и инвесторов;
- увеличиваются налоговые поступления в регионы;
- появляются новые рабочие места.

Формирование высокоэффективных индустриальных кластеров значительно ускорилось бы с помощью крупных целевых инвестиций. Богатая сырьевая база – основа для интеграции многих важнейших отраслей, таких как машиностроение, производство транспортного оборудования, химическая, целлюлозно-бумажная промышленность и полиграфия. Кластеры могут формироваться на региональной основе, где наблюдается высокая географическая концентрация взаимосвязанных отраслей[1,3].

Использование кластерных технологий наиболее перспективно на тех территориях, где бизнес и власть намерены создать конкурентоспособную отрасль промышленности. Используя преимущественно горизонтальные связи, специализацию и качественные ресурсы, инновационные кластеры получают возможность для достижения более высоких результатов.

Отличительная черта кластера – целевая предпринимательская деятельность. В рамках кластера объединяются не только производственный, но и инновационный бизнес, комплексное управление качеством продукции, сервисное обслуживание. Объединение усилий предпринимателей, органов управления, субъектов инвестиционной и инновационной деятельности на определенной территории дает значительные преимущества в конкурентной борьбе. Внедрение кластерных технологий объединения предприятий способствует росту деловой активности предпринимательских структур, улучшению инвестиционного климата в регионе страны, развитию социальных, экономических, информационных и интеграционных систем.

Исследование показало, что многие инновационные кластеры сформированы на базе бывших советских предприятий из передовых по технологиям в советской экономике отраслей – электроника, авиа- и ракетостроение, химическая промышленность, ядерные технологии. Примером такого кластера является Инновационно-технологический кластер «Южное созвездие», созданный в Ростовской области в 2015г.

Основной целью создания кластера являлась консолидация на принципах государственно-частного партнерства производственного, научно-образовательного, инновационного, организационного, административного потенциала организаций-участников кластера, направленная на повышение конкурентоспособности выпускаемой продукции и региональной экономики в целом [2]. Ядром кластера стали ТАНТК им. Г.М. Бериева, ОАО «Гранит», ОАО «Алмаз», ОАО «Азовский оптико-механический завод», ОАО «НПП КП «Квант».

Структуру органов управления кластером можно представить на рис.1:

Функции органов Управления:

1. Функции Собрания участников Кластера:

Собрание участников Кластера принимает решения по вопросам:

- разработки стратегии развития Кластера;

Рис.1 Состав организаций в структуре кластера

- утверждения программ развития Кластера;
- утверждения отчетов специализированной организации Кластера;
- иным вопросам, выносимым на обсуждение специализированной организацией Кластера или по инициативе участников Кластера [4].

2. Функции специализированной организации Кластера:

Специализированная организация Кластера является участником Кластера и осуществляет, в том числе, следующие функции:

- выявляет общие интересы участников Кластера посредством проведения с ними встреч, переговоров, совещаний, конференций и иными способами;
- координирует развитие внутри кластерных инициатив и разработку программ и проектов в интересах отдельных участников или группы участников Кластера, при необходимости выносит их на рассмотрение Собрания участников Кластера;
- участвует в разработке программы развития Кластера и выносит ее на обсуждение собрания участников Кластера, ежегодно готовит предложения по необходимым изменениям отдельных ее положений, включению программ и проектов;
- совместно с заинтересованными сторонами участвует в разработке предложений по трансферу технологий, управленческих и инновационных решений между участниками Кластера и иными лицами, совместному партнерству в инновациях и производстве, информационному обмену;
- оказывает содействие участникам кластера в выводе на рынок новых продуктов (услуг), развитии кооперации организаций – участников в научно-технической сфере, в том числе с иностранными организациями;
- организует выставочно-ярмарочные и коммуникативные мероприятия в сфере интересов участников Кластера, а также их участие в выставочно-ярмарочных и коммуникативных мероприятиях, проводимых в России и за рубежом;
- оказывает содействие в подготовке, переподготовке, повышении квалификации и стажировке кадров, предоставляет консультационные услуги в интересах участников Кластера;
- представляет интересы участников Кластера в отношениях с третьими лицами по вопросам, направленным на достижение коммерческого результата.

Схему взаимодействия организаций внутри кластера и с внешней средой можно представить следующим образом (рис.2)

Рассмотрим подробнее реализацию некоторых инновационных разработок данного кластера [3, 5]:

Автоматизированная система контроля и учета энергоресурсов «Квант-Энерго»

Данная система представляет собой программно-аппаратный комплекс, обеспечивающий учет потребления энергоресурсов и воды промышленными предприятиями и объектами ЖКХ.

Система основана на беспроводной технологии удаленного сбора данных с энергетической автономностью компонентов системы. Система позволяет осуществлять контроль и мониторинг состояния счетчиков и передавать информацию (в том числе архивные показания и сведения об инцидентах/вмешательствах) с приборов учета энергоресурсов и воды информации в информационные системы ресурсоснабжающих организаций, в ГИС ЖКХ, а также в личные кабинеты пользователей, руководителям ТСЖ, СНТ и управляющих компаний.

Разработка данной системы была полностью за-

Рис. 2. Взаимодействие организаций внутри кластера и с внешней средой

вершена и в настоящее время Система учета энергоресурсов «Квант-Энерго» включена в Единый реестр российских программ для электронных вычислительных машин и баз данных (приказ Минкомсвязи России от 05.07.2018 №347) Рег.№ 4593 от 05.07.2018

Биометрическая система авторизованного доступа FACEIDENT.

Система ФэйсИдент предназначена для идентификации персоны по изображению лица. Она реализована в виде программного модуля, который может использоваться независимо, или в комплексе с другими программно-аппаратными средствами, например — системами видеонаблюдения, авторизации.

Предлагаемая система востребована во многих областях. Например, её использование в офисных помещениях, во-первых, позволит заменить механические ключи на биометрические, которые невозможно утерять и сложнее подделать, во-вторых, предоставит удобный инструментарий для автоматического учёта рабочего времени сотрудников. Применение ФэйсИдент в сфере оказанию услуг позволит заранее распознать постоянного клиента, использовать индивидуальный подход, адаптируя услуги с учетом предыдущих заказов. Разработанный комплекс может быть тиражирован для использования в системах информационной защиты и санкционированного допуска.

Аппаратно-программный комплекс «ВОСХОД»

Комплекс технических средств «Восход» предназначен для координации действий аварийно-спасательных служб и медицинского персонала и принятия первичных решений по сортировке пострадавших на до госпитальном этапе оказания медицинской помощи в зоне ведения боевых действий и чрезвычайных ситуаций. В рамках этого проекта создается экспертная автоматизированная персональная система в виде мобильных устройств, связанных с центральной станцией на автомобильном шасси, обеспечивающая поддержку принятия решения каждому из спасателей медицинской службы на этапах оказания неотложной помощи на месте происшествия и транспортировку по назначению в лечебные учреждения.

Информационно-телекоммуникационный комплекс спутниковой навигации ГЛОНАСС/GPS/GALILEO.

Комплекс предназначен для отслеживания происходящих в реальном времени событий, связанных с передвижением транспорта, перемещением особо важных грузов, перевозкой людей, контролем норм труда и отдыха водителей транспортных средств, обеспечением безопасности людей и грузов; оповещения медицинских, дорожно-патрульных и аварийных служб о дорожно-транспортных происшествиях (ДТП). В состав комплекса входит система оценки психофизиологического состояния

водителя.

Однако несмотря на высокий уровень достигнутых разработок, у кластера наблюдается явный разрыв между высоким качеством инновационной продукции и низким объемом ее реализации на рынке. Во многом это объясняется тем, что рынок инновационной продукции радикальным образом отличается от традиционного, и к нему не применимы методы классического маркетинга. В связи с этим кластеру важно уделить особое внимание налаживанию сбыта своей продукции, в частности, как созданию собственного технологического брокера, так и сотрудничеству со сторонними центрами трансфера технологий.

Заключение. Таким образом, для развития инновационных кластеров в России характерны две большие проблемы – небольшая доля частного финансирования и разрыв между высоким качеством инновационной продукции и низким объемом ее реализации на рынке.

Решение проблемы увеличения доли частного финансирования возможно

во-первых, в установлении особых льготных налоговых режимов для инновационных кластеров, а во-вторых, в создании инфраструктуры для привлечения частного капитала, в том числе иностранного. Проблема сбыта инновационной продукции может быть решена как через стимулирование сбыта посредством государственного заказа, так и с помощью специализированных компаний, занимающихся маркетингом инновационной продукции – технологических брокеров и центров трансфера технологий.

Список литературы

1. Портер М., 2005, Конкуренция. : Пер. с англ. – М.: Издательский дом «Вильямс».
2. Устинова Л.Н. Особенности развития промышленности в условиях цифровизации./ Монография «Формирование цифровой экономики и промышленности. Новые вызовы.Глава 3 /под редакцией д.э.н, проф. Бабкина.-СПб 2018, с.176-197.
3. Обзор инновационных кластеров в иностранных государствах. Миэкономразвития России. Май 2011г.
4. Клейнер Г., Бабкин А. формирование телекоммуникационного кластера на основе виртуального предприятия //конспекты лекций по информатике (включая подсерии конспект лекций по искусственному интеллекту и конспект лекций по биоинформатике). Т. 9247. 2015. С. 567-572.
5. Устинова Л.Н. «Индустрия 4 –новые вызовы для российского производства» / коллективная Монография по материалам научно-практической конференции «Цифровая экономика и ИНДУСТРИЯ 4» разд.1, Стр.81-87. 2018.

ОБЕСПЕЧЕНИЯ НОВОГО РЕСУРСА «ИНФОРМАЦИЯ» НА ПРЕДПРИЯТИИ

Гулид Анатолий Константинович
Тестировщик-Технический писатель, аэропорт Домодедово

Аннотация: *в данной статье рассматривается понятия как информация, информационная безопасность в компании, основные угрозы от мошенников и основные рекомендации к защите информации.*

Ключевые слова: *информация, угроза, информационная безопасность, информационные технологии, предприятие.*

Abstract: *this article discusses the concepts of information, information se-curity in the company, the main threats from fraudsters and the main recommen-dations for the protection of information*

Keywords: *information, threat, information security, information technolo-gies, enterprise.*

Введение. В век цифровых технологий, который развивается достаточно быстро, Информация всегда играла чрезвычайно важную роль в жизни человека. Вспоминается простая фраза «Тот, кто владеет информацией, тот владеет и миром». Следует отметить, что исключительная роль информации в современном мире привела к пониманию информации как ресурса, столь же необходимого и важного, как энергетические, сырьевые, финансовые и другие ресурсы. Информация стала предметом купли - продажи, т.е. информационным продуктом, который наравне с информацией, составляющей общественное достояние, образует информационный ресурс общества. В результате научно-технического прогресса человечество создавало все новые средства и способы сбора, хранения, передачи информации. Но важнейшее в информационных процессах является обеспечение защиты информации. Почти везде можно услышать простое понятие, которое связано с защитой

информации – «Информационная безопасность». Информационная безопасность создает условия формирования безопасного состояния информации и ее использование. Самый простой и очевидный пример – это мобильные телефоны, а точнее обеспечение защиты информации, которая хранится на телефоне, где самый простой пример защиты – это пароль. Многие не задумываются о полной защите и используют свою технику без паролей, что делает их технику уязвимой. В последнее время стало популярным использовать вместо паролей сканер отпечатков пальца или «Face ID»- сканирование лица, что не требуют в настройке большого времени[1].

В банках, например хранится вся информация об клиентах, потеря информация или простая утечка информации может помочь злоумышленникам получить все, что они хотят: начиная от фамилии клиента и заканчивая местом жительства, а более опытные злоумышленники могут получить не только эту информацию, но и доступ к вашим картам – деньгам.

Цель исследования: Аналитический анализ обеспечения безопасности персональных данных на предприятии.

Задачи исследования:

Проанализировать структуру информационной безопасности.

Рассмотреть законодательную базу по защите персональных данных.

Почти каждое предприятие располагает различными видами информации, представляющими интерес для злоумышленников. Прежде всего, это коммерческие данные, информация, являющаяся интеллектуальной собственностью предприятия и конфиденциальные данные. В стабильной компании, защита своих информационных систем, создает надежные и безопасные условия для работы. Утечки, отсутствие и кражи информации всегда влияет на состояние компании.

На данный момент есть три основных момента, которые должна соблюдать информационная безопасность[2]:

- целостность данных – обеспечение защиты достоверности и целостности информации

- доступность для пользователя – каждый вид информации должен быть открыт для чтения определенному кругу сотрудников. Тут стоит понимать, что из-за большого вида информации, которая хранится в компании, нужно строго понимать границы доступа.

- обеспечение недопустимости угроз повреждения и утраты информации - защиту непосредственно от угроз целенаправленного уничтожения или повреждения информации

Существует два основных вида угроз для информации

Первый вид угроз связан с хакерами и атаками вирусов. Данный вид угроз нацелен на кражу или порчу информации, что может привести к частичной или даже к полной потере информации. Такое действие может привести к частичной или полной остановке работы на предприятия с дальнейшими последствиями или убытками.

Второй вид угроз – это сотрудники предприятия. Тут можно выделить два типа деятельности по потери информации. Первый зависит от сотрудника, который обеспечивает саму информационную безопасность. Он должен своевременно обновлять программное обеспечение для защиты информации, производить резервное копирование для восстановления и следить за самим оборудованием, на котором хранятся все виды информации. С помощью определенных программ сотрудник информационной безопасности и обеспечивает доступ к нужной информации, которую использует пользователь, но и обеспечивает

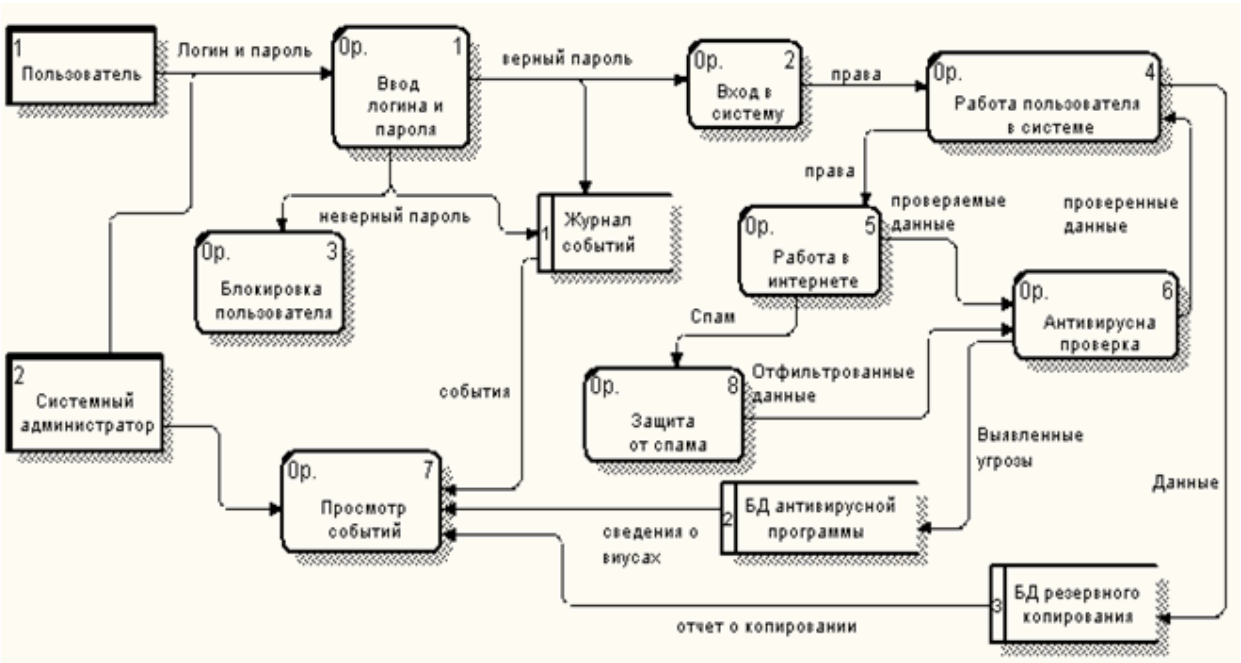


Рисунок 1. Структура информационной безопасности

защиту предоставляемой информации. На Рисунке 1 можно увидеть последовательность действий простого пользователя предприятия, где нужно учитывать доступ и безопасность информации.

Второй тип - это недовольные сотрудники, сотрудники «Шпионы», которые могут предоставить информацию третьим лицам, что может создать не мало проблем для предприятия. Тут уже влияет человеческий фактор. Для устройства на работу многие предприятия, для нового сотрудника, проводят множество мероприятий, которые помогают понять, что за человек к ним устраивается. Это может быть обычная беседа с психологом или даже прохождение полиграфа, что сразу показывает настрой и важность самого предприятия[4].

Переходя к рассмотрению вопросов защиты персональных данных, следует отметить, что они остаются неизменно острыми на протяжении последних лет и поднимаются в самых высоких кабинетах как в России, так и за рубежом, поскольку касаются каждого из нас, вне зависимости от гражданства и должности. С приходом информационных технологий защита личных данных стала еще более актуальной. В Федеральный Закон вносились изменения, основные из которых были введены 261-ФЗ от 25.07.2011 и 242-ФЗ от 21.07.2014. Первый закон внес существенные изменения в базовые постулаты защиты ПДн, а второй запретил первичную обработку ПДн за пределами территории РФ.

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. законы, которые относятся к сфере информационной безопасности[3]:

- Федеральный закон №152 «О персональных данных». ФЗ регулирует отношения между органами государственной власти во время поиска важных сведений и обеспечивает информационную безопасность персональных дан-ных

- Федеральный закон №63 «Об электронной цифровой подписи». ФЗ перечисляет области деятельности, в которых используется электронная циф-ровая подпись в целях обеспечения информационной безопасности. Напри-мер, покупка товаров, оказание услуг и т.д.

Федеральный закон «Об информации, информационных технологиях и о защите информации» был принят Государственной Думой 8 июля 2006 го-да, а одобрен Советом Федерации спустя 6 дней того же года. Последние из-менения были внесены 27 июля 2017 года.Государство также определят меру ответственности за нарушение положений законодательства в сфере ИБ. Например, глава 28 «Преступления в сфере компьютерной информации» в Уголовном кодексе Российской Федерации, включает три статьи:

- статья 272 «Неправомерный доступ к компьютерной информации»;

- статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;

- статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»

Вывод: Информация в настоящее время приобрела коммерческую ценность, стала продуктом и товаром, которая важна для успешного развития предприятия, поэтому она нуждается в защите. Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные как маленького так и большого предприятия.

Список литературы

1. Алехина Г.В. Информационные технологии в экономике и управлении / Московский международный институт эконометрики, информатики, финансов и права. - М.: 2014. - 238 с.
2. Буга В.Д. Информационная безопасность на предприятии: что ей угрожает? средства защиты в сфере информационных технологий: какой антивирус наиболее эффективен // Молодежный научный форум: Технические и математические науки: электр. сб. ст. по мат. XI междунар. студ. науч.-практ. конф. №4.
3. Федеральный закон «О персональных данных» N 152-ФЗ от 27.07.2006 (ред. от 31.12.2017) // URL: http://www.consultant.ru/document/cons_doc_LAW_61801/
4. Драга А.А. Обеспечение безопасности предпринимательской деятельности. – М.: Издательство МГТУ им. Н. Э. Баумана. 2014. – 304 с.

ОРГАНИЗАЦИЯ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА В ВУЗАХ РФ

Галкова Екатерина Александровна
Специалист отдела технической защиты информации
ООО «Лоджикал АйТи»

Даньшина Марина Владимировна
Заместитель декана факультета Информационных технологий
Московского политехнического университета

Аннотация: *В статье рассмотрена организация системы контроля до-ступа на предприятие. Рассмотрены методы защиты обеспечения безопасно-сти на предприятии и разработаны рекомендации по усовершенствованию данной системы.*

Ключевые слова: *обеспечение безопасности, предприятие, информа-ционные технологии, СКУД.*

Abstract: *The article describes the organization of the access control system in the enterprise. Examines the methods of ensuring security in the enterprise and recommendations for an improved system.*

Keywords: *security, enterprise, information technology, access control.*

Введение. В современном мире информация очень важна на любом предприятии. Большую роль в деятельности организации играет эффективное использование информации, ее безопасное хранение и передача, так как все это сказывается на прибыли и развитии предприятия. Сейчас большинство документов и данных представлены в электронном виде, что удобно, но в тоже время очень небезопасно. Комплексная система защиты информации (КСЗИ) – представляет собой организационные и инженерно-технические мероприятия для защиты информации от нарушения целостности, конфиденциальности и доступности.

Современные вузы владеют большим объемом данных, которые содержат разнообразную информацию такую как: персональные данные учащихся, преподавателей и иных сотрудников, учебные планы, финансовые документы, важные документы по проектам и исследованиям. Вузы являются небезопасными объектами, так как они являются публичными помещениями, в которых преобладает непостоянная аудитория.

Цель исследования: Проанализировать безопасность системы контроля доступа в вузах РФ.

Задачи исследования:

Изучить системы контроля доступа на предприятие и их организацию.

Определить важность обеспечения защиты безопасности в вузе.

Рассмотреть методы обеспечения защиты безопасности в вузе.

Система контроля и управления доступом (СКУД) это система, состоящая из программно-технического оборудования и ряда мероприятий, проводимых для автоматизации пропуска сотрудников на территорию защищаемого объекта. [1]

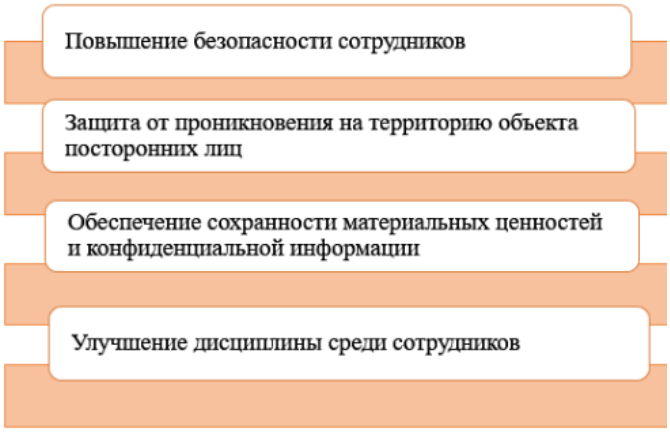


Рисунок 1. Причины установки СКУД на предприятии

Причины внедрения системы контроля и управления доступом на предприятие представлены на рисунке 1.

При формировании СКУД выделяют точки и зоны доступа. Точки доступа — это места, где проверяется идентификатор пользователя на право этого лица находиться на охраняемом объекте. В качестве идентификатора могут выступать: ключи, карточки и коды. Точки доступа представляют собой турникеты, шлагбаумы, двери, которые оснащены специальными замками. В зависимости от требований к безопасности и расположения на объекте охраняемых помещений такие точки доступа могут находиться в различных местах защищаемой территории. [2]

Системы контроля и у правления доступом, установленные в помещениях дают возможности, представленные на рисунке 2.

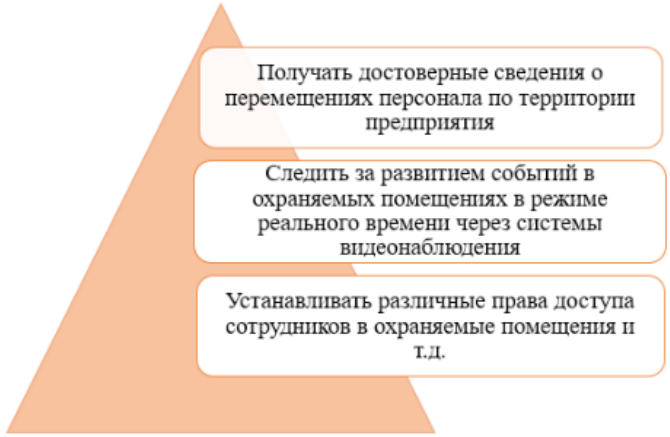


Рисунок 2. Возможности СКУД

Системы контроля и у правления доступом востребованы во многих отраслях. На рисунке 3 отображено, где наиболее востребованы СКУД:

В работе СКУД используются компоненты, которые представлены на рисунке 4.

В зависимости от масштабов защищаемого объекта сложность и размер внедряемой системы контроля доступа могут варьироваться.

Одна из самых важных задач в организации и внедрении СКУД в систему вуза - использование информационных технологий. Во-первых, это необходимо для выполнения требований криминальной безопасности, так как в стране наблюдается рост преступности и угроз террористических актов. Во-вторых, необходимо запретить проход посторонних в ряд помещений, а также вести учет рабочего времени и контролировать посещаемость студентов в реальном времени. Кроме того, вузы, использующие современные информационные технологии, имеют высокий престиж.

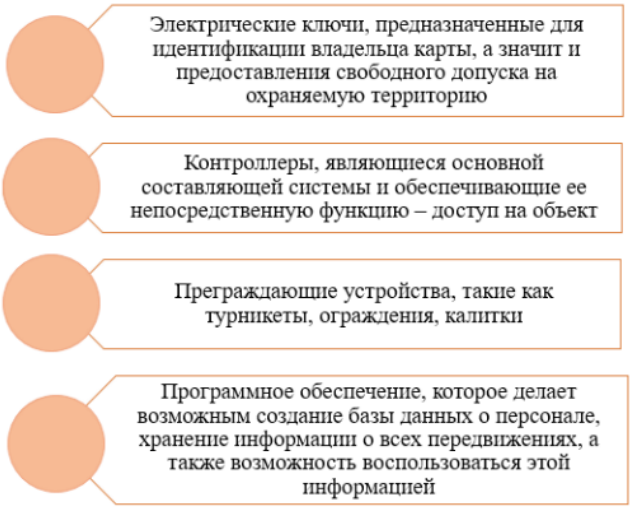


Рисунок 4. Компоненты СКУД

Каждый сотрудник и учащийся имеет свой уникальный идентификатор. Он позволяет проходить на территорию вуза, а также проходить в некоторые помещения с ограниченным допуском. [3]

Наиболее часто идентификатор имеет форму пластиковой карты с магнитной полосой, на которую записана персональная информация сотрудника или учащегося. Чтобы получить доступ на территорию или в помещение для ограниченного количества лиц, собственник карточки должен поднести ее к считывающему устройству, после чего контроллер позволяет ему пройти на охраняемый объект. Тем не менее такой идентификатор может замедлять проход на территорию с большим числом сотрудников и учащихся, так как на прикладывание карты уходит некоторое время. В этом случае можно использовать современные радиочастотные бесконтактные Proximity-карты или брелоки Touch Memory, кото-

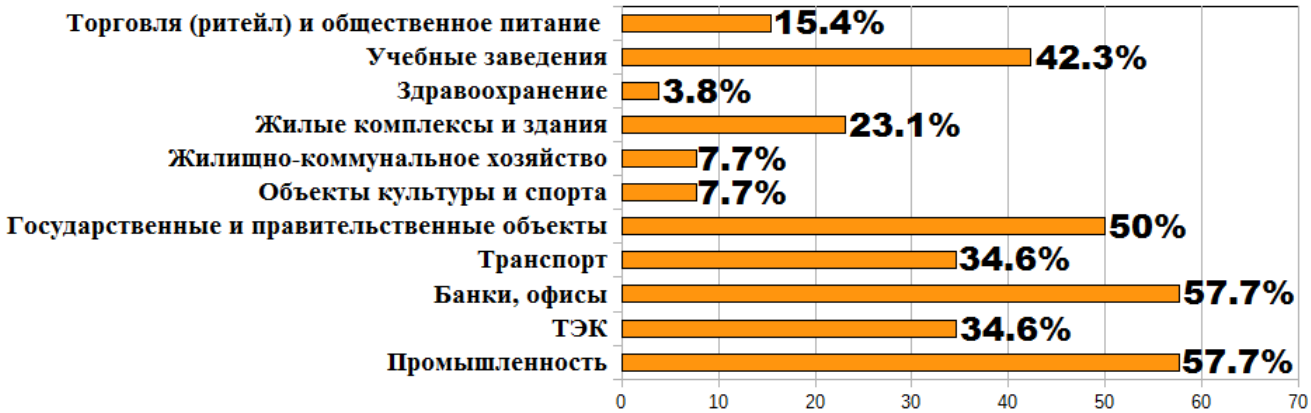


Рисунок 3. Востребованность СКУД в отраслях

рые представляют собой металлическую таблетку с чипом внутри. В новых системах контроля доступа используется дополнительная идентификация по фото владельца. Наиболее часто сегодня применяются биометрические сканеры отпечатков пальцев, картридеры и клавиатуры для набора ПИН-кода.

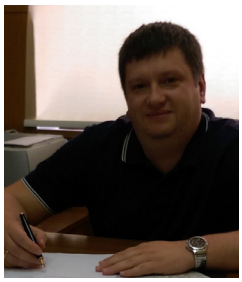
Вывод. СКУД стали частью современной корпоративной культуры. С помощью системы контроля и управления доступом решается достаточно много задач: создание пропускного режима на территорию вуза, в аудитории, лаборатории, другие помещения с ограниченным доступом, а также в общежития, учет рабочего времени преподавателей, контроль посещаемости студентов. Внедрение такой системы является дополнительным гарантом безопасности вуза, что очень важно в современном мире.

Список литературы

1. Тюменев А.В. Обеспечение безопасности информационных ресурсов предприятия/Тюменев А.В., Панов Н.Н./Системные технологии. 2017. № 3 (24). С. 68-71.
2. Системы контроля и управления доступом (СКУД) http://www.prom-seti.ru/lmenu/sistemy-kontrolya-i-upravleniya-dostupom-skud/
3. Александр Красноцветов Особенности создания СКУД в вузах/ ТЗ №3-2010 г.

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Вершинина Дарья Дмитриевна
Специалист отдела технической защиты информации
ООО «Лоджикал АйТи»



Тюменев Александр Владимирович
Подполковник полиции, начальник управления комплексной безопасности Московского политехнического университета

Аннотация: *В статье рассмотрено комплексное обеспечение безопасности предприятия. Особое место уделено физическим методам защиты. Рассмотрены механизмы, используемые для защиты контролируемой зоны организации. Использование комплексной системы позволяет успешно функционировать в нестабильных условиях внешней и внутренней среды.*

Ключевые слова: *безопасность, информационная безопасность, защита, методы.*

Abstract: *This article describes the comprehensive security of the enterprise. A special place is given to physical methods of protection. The mechanisms used to protect the controlled area of the organization are considered. The use of an comprehensive system allows you to successfully operate in unstable condi-tions of external and internal environment.*

Keywords: *security, information security, protection, methods.*

Введение. В современном мире важнейшим ресурсом является информация. Множество предприятий каждый день обрабатывают данные различных видов, которые несут огромную значимость для компании. Информационную безопасность предприятия определяет используемая им информационная технология, являющаяся в виде информационного процесса, производимого на рассортированных по контролируемой зоне организации технических средств; а также наличие мест доступа или утечки информации, создающих потенциальную возможность осуществления угроз; и наличие действенных средств защиты. Одной из наиболее важных составляющих комплексной безопасности организации является физическая защита.

Цель исследования: Изучить обеспечения безопасности предприятия.

Задачи исследования:

- Проанализировать обеспечение безопасности на предприятии России.
- Рассмотреть физическую безопасность предприятия.
- Разработать рекомендации по усовершенствованию комплексной безопасности на

предприятии.

Главной целью комплексной системы защиты информации является обеспечение непрерывности бизнеса и предотвращение угроз его безопасности. Для непрерывной работы предприятия необходимо защищать информационную систему от возникающих угроз, чаще всего угрозой является физическое лицо и его действия в отношении информационной системы, последствия которых могут быть катастрофическими. Примером этого является: хищение имущества или персональных данных, а также создание непредвиденных ситуаций на объекте. На базе принципов «разумной достаточности», «эффективность – стоимость» строится безопасность любой организации, также она должна базироваться на тщательно проработанной концепции физической безопасности на предприятии. Согласно статистике больше 80% организаций подвержены нарушениям безопасности данных, что привело к финансовым убыткам. [1]

Анализируя информационные атаки можно выделить слабые места в обеспечении безопасности информационных ресурсов предприятия. Наиболее встречаемая это утечка информации к конкурентам, потеря данных, передача в чужие руки конфиденциальной информации компании – все это несет большой риск для предприятия. Результаты исследования представлены на рисунке 1.

Физическая безопасность (защиты) организации – это совокупность правовых норм, организационных мер и инженерно-технических решений, направленных на защиту важных интересов и ресурсов предприятия (объекта) от угроз злоумышленных противоправных действий физических лиц (нарушителей). [2]

Методы защиты представлены на рисунке 2.

Препятствие – данные средство подразумевает использование физических барьеров для защиты информации от мошеннических действий. Реализуется путем запрета к носителям информации и аппаратуре.

Маскировка – способ защиты информации, использующий шифрование данных в автоматизированной системе (АС).

Управление доступом - метод, базирующийся на разграничении доступа к информации. Позволяет регулировать степень доступа в зависимости от выполняемых функций в организации.

Регламентация – метод, предполагающий, что при незаконном запросе злоумышленника доступ к хранению и передаче данных будет минимален.

Побуждение - метод, основанный на принятых в обществе правилах, стимулирующий не нарушать запрет на использование конфиденциальной информации.

Принуждение – метод, обязывающий пользователей при доступе к конфиденциальной информации соблюдать определенный регламент (правила). Нарушение влечет материальную, административную или уголовную ответственность.

Рисунок 2. Методы физической защиты информации

Выше описанные методы защиты обеспечивают максимальный уровень безопасности всей информационной системы предприятия.

Рассмотрим один из защитных механизмов:

Физические средства защиты нужны для качественной организации внешней охраны и наблюдения за контролируемой зоной, а также для защиты автоматизированной информационной системы. На предприятии представлены в виде специальных технических устройств.

Структурная схема типовой системы физической

Рисунок 1. Атаки на предприятие

защиты приведена на рисунке 3.

Рисунок 3. Система физической безопасности предприятия

Обычно в организации используются механические системы. Наряду с ними внедряются электронные АС физической защиты. Под электронной системой понимается защита территории объекта, пожарная безопасность, охрана помещений, пропускной режим, наблюдение и устройства сигнализации.

После анализа уязвимостей объекта, которые являются важнейшей задачей на стадии проектирования, следует разработать рекомендации по обеспечению безопасности.

Для предотвращения несанкционированного доступа к защищаемой информации через электромагнитные каналы используют специальные устройства и материалы, которые обладают свойствами поглощать и предохранять от посторонних воздействий:

- Экранирование всех поверхностей в помещении – пола, стен и потолка с помощью металлизированных панелей.
- Оконные проемы оборудуют жалюзи с металлической нитью или покрывают стекла токопроводящим составом;
- На все отверстия в помещениях устанавливают металлические сетки с системой заземления или соединяют с настенной экранировкой;
- В вентиляционные каналы устанавливают аудиоизлучатели, блокирующие распространение радиоволн;
- Применяют шумовые генераторные устройств для предотвращения утечки информации по каналам ПЭМИН (Побочные электромагнитные излучения и наводки), а также для защиты от закладных подслушивающих устройств.

Защита всего информационного оборудования организации, а также переносных устройств (магнитных лент или флеш-накопителей) осуществляется с помощью механизмов изображенных на рисунке 4:

Рисунок 4. Механизмы защита информационного оборудования и переносных устройств

- Замки (механические, радиоуправляемые, кодовые, с чипом), которые желательно поставить на сейфы, системные блоки, оконные блоки, двери и другие устройства;
- Инерционные датчики - используются в электросети, телефонных проводах, телекоммуникационных антеннах, который искажает частоту измеряемого сигнала;
- Микровыключатели - устройства дистанционного управления, которые фиксируют открывание и закрывание окон и дверей;
- Акустомагнитные этикетки/наклейки - приклеивают на приборы, документы, системные блоки, узлы для защиты от выноса за контролируемую зону организации или помещения. При попытке выноса злоумышленником документов или устройств, имеющих данную этикетку, через пропускные устройства звучит сигнал тревоги.
- Специальные сейфы и шкафы из метала, в которые устанавливают серверы, принтеры и другие переносные устройства.

Схема использования механизмов защиты приведена на рисунке 5.

Блоки и узлы автоматизированной системы требуют особой защиты. Для это применяют:

- Экранированный кабель, который будет монтироваться внутри и снаружи стен;

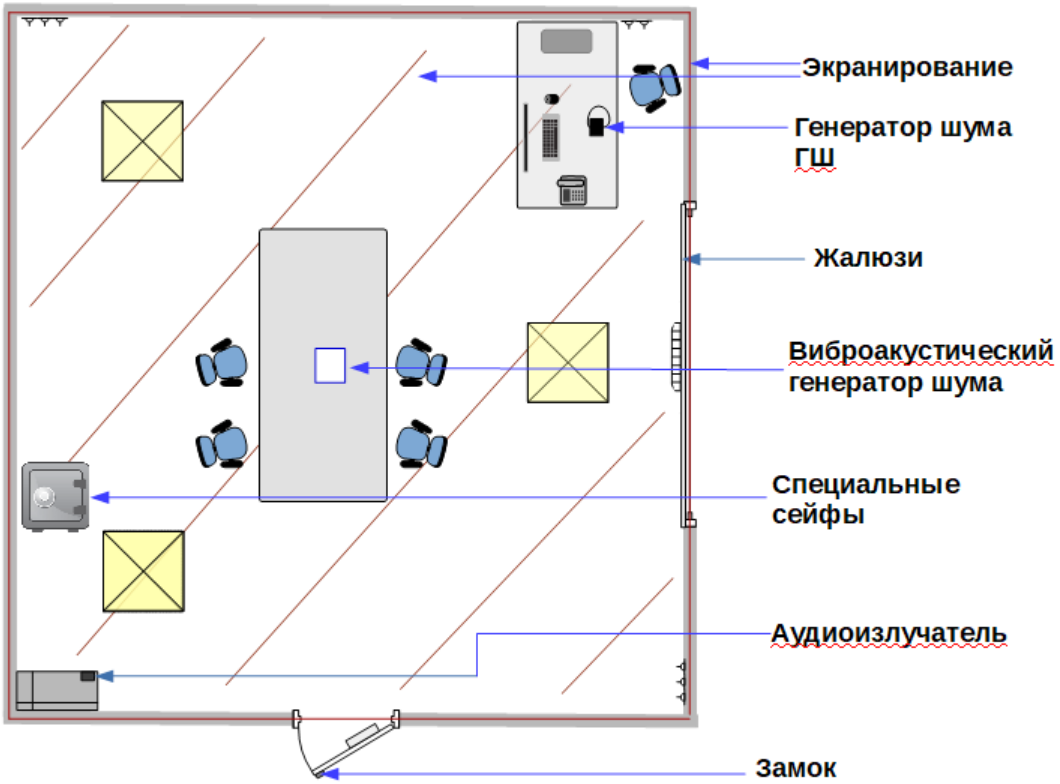


Рисунок 5. Схема помещения

- Сетевые фильтры, которые не пропускают электромагнитные излучения;
- Провода, дроссели, наконечники, конденсаторы и другие устройства, которые имеют помехоподавляющее действие;
- Диэлектрические разделительные вставки, которые устанавливают на водопроводные и газовые трубы для разрывания электромагнитной цепи.

Не все описанные методы являются оптимальными:

- Для обнаружения подслушивающих устройств самым продуктивным является использование рентгена. Рентгеновское обследование имеет и свои минусы: оно самое дорогостоящее, а также наносит вред здоровью человека.
- Генераторы шума, действующие методом снятия излучений с дисплея, также отрицательно сказываются на здоровье. Таким образом, данное устройство защиты применяется достаточно редко на практике.

Вывод. В условиях современного рынка необходимо внедрять все выше описанные методы и механизмы защиты для предотвращения несанкционированных угроз безопасности. Способы и виды взломов и нападений на конфиденциальные данные постоянно совершенствуются и поэтому необходимо регулярно проверять и обновлять защитную систему предприятия и быть в курсе новых угроз и методов борьбы с ними.

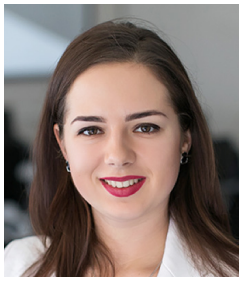
Список литературы

1. Тюменев А.В. Обеспечение безопасности информационных ресурсов предприятия/ Тюменев А.В., Панов Н.Н.// Системные технологии. 2017. № 3 (24). с. 68-71.
2. В. Л. Шульц, А. Д. Рудченко, А. В. Юрченко. Безопасность пред-принимательской деятельности/ Учебник для академического бакалавриа-та// М. : Издательство Юрайт, 2017. — 237 с.

РАЗДЕЛ III. ПРОЕКТИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СФЕРЕ

ЦИФРОВИЗАЦИЯ КАК ФАКТОР РАЗВИТИЯ НОВОЙ МОДЕЛИ БАЛАНСА СЕМЬЯ-РАБОТА

Разумова Татьяна Олеговна
доктор экономических наук, профессор, заведующий кафедрой экономики труда и персонала экономического факультета МГУ имени М.В. Ломоносова



Серпухова Мария Александровна
ассистент кафедры экономика труда и персонала МГУ имени М.В. Ломоносова

Аннотация: *В статье рассматривается влияние цифровизации на достижение баланса семья-работа как ключевого индикатора концепции Международной организации труда «Достойный труд». Авторы выявляют как новые возможности для благоприятного сочетания работы и личной жизни благодаря информационным технологиям, так и возникающие риски. Предложены меры, направленные на преодоление рисков и обеспечение повышения качества жизни населения.*

Ключевые слова: *рынок труда, цифровизация, баланс семья-работа.*

Abstract: *The article examines the impact of digitalization on the achievement of family-work balance as a key indicator of the concept of the international labour organization «Decent work». The authors identify both new opportunities for a favorable combination of work and personal life thanks to information technology, and emerging risks. The measures aimed at overcoming risks and improving the quality of life of the population are proposed.*

Keywords: *labor market, digitalization, family-work balance.*

В современных условиях одной из наиболее актуальных задач для Российской Федерации является переход на качественно новый, инновационный путь развития. При этом, на конституционном уровне в нашей стране закреплен постулат о социальном государстве: «Российская Федерация – социальное государство, политика которого направлена на создание условий, обеспечивающих достойную жизнь и свободное развитие человека» [3]. Для реализации данной функции Российская Федерация руководствуется основными принципами концепции устойчивого развития, целью которой является повышение качества жизни населения, что в свою очередь предопределяется благоприятным соотношением работы и личной жизни.

Вопросы взаимосвязи между оплачиваемой трудовой деятельностью и возможным ее влиянием на выполнение семейных обязательств в различные времена входили в круг интересов таких авторов, как: Г. Беккер [6], Р. Гронау [9], Д. Дойран и Г. Калб [8] , А. Бут [7] и др. Современные российские исследования, посвящённые изучению проблемных аспектов совмещения семьи и работы, представлены в трудах И.Е. Калабихиной [2], А.Л. Синицы [4], Г.Ф. Хуснутдиновой и Е.М. Воробьева [5] и др.

Создание условий для совмещения семейных функций и трудовой деятельности работников в контексте поиска баланса между исследуемыми категориями на современном рынке труда является одной из приоритетных задач Международной Организации Труда (МОТ). Концепция «Достойный труд», которая была сформулирована МОТ в 1999 году, создает основные стимулы для достижения баланса между работой и выполнением семейных обязательств.

Проведенный комплексный анализ ключевых индикаторов реализации концепции «Достойный труда» в их взаимосвязи с наличием у работников семейных обязательств позволил сделать вывод о том, что достижение равновесия между рабочими обязательствами и семейными функциями является принципиально важным вопросом для большинства

трудящегося населения России: доля занятых, состоящих в брачных отношениях, за последние 5 лет увеличилось более чем на 3 млн чел. При этом более половины безработных имеют семьи. Важно отметить, что существует сильная корреляционная зависимость между уровнем безработицы и наличием у данной категории рабочей силы супруга или супруги: чем выше уровень безработицы, тем менее склонны безработные оставаться в семейных отношениях, и наоборот.

Одной из проблем современного рынка труда является значительный рост количества молодежи, которая не учится и не работает в общей численности населения возрастной группы от 15 до 24 лет – с 11,8% в 2012 г. до 12,4% в 2015 г. Такая тенденция может быть связана с растущими возможностями молодого поколения использовать современные технические средства в целях получения дистанционного образования или удаленной работы.

По данным результатов развернутого опроса Kelly Global Workforce Index [1], проведенного в декабре 2014 - феврале 2015 года, более 64% респондентов из России считают наличие возможностей для удаленной работы и гибкого графика ключевым элементом для достижения баланса между семьей и работой. Создание условий для достижения этих показателей, как на уровне общества в целом, так и в масштабах отдельного домохозяйства, возможно за счет цифровизации.

При этом важно понимать, что в условиях создания новых возможностей, могут возникать и новые риски, как для рынка труда, так и для социальной среды, трансформируя устоявшиеся методы для достижения равновесия между семейными и рабочими функциями. В условиях новых технологий и цифровизации происходит активное стирание границ между работой и личной жизнью: хранение рабочей информации в сети и быстрый доступ к ней дает возможность работникам осуществлять свои трудовые обязательства на удаленном рабочем месте, не присутствуя в офисе. С другой стороны, возникают риски ненормируемого рабочего дня, когда задания могут приходить в различное время, а наличие нетрудовой обстановки в месте работы создает множество препятствий для полноценного выполнения оплачиваемой деятельности.

Несмотря на то, что в нашей стране создаются определенные предпосылки для достижения баланса семья-работа, необходимым представляется разработка комплексного механизма поддержки отдельных категорий занятого населения на основе принципиально новых нормативно-правовых документов, регулирующих социально-трудовые отношения в условиях цифровизации экономики, при которой происходит все большее стирание границ между работой и личными ролями.

Список литературы:

1. Выбирая между работой и личной жизнью // Kelly Global Workforce Index – Электронный ресурс. – https://www.kellyservices.ru/ru/about-company/workforce-trends1/kgwi-2016-01/ (дата обращения: 30.03.2019).
2. Калабихина И.Е. Гендерная дискриминация на российском рынке труда: современная ситуация и актуальные предложения по устранению неравенства // Проблемы правовой защиты женщин от дискриминации в сфере труда и занятости. – М.: Консорциум женских неправительственных организаций, 2008. – 190 с.
3. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) / С учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) – Электронный ресурс. – http://www.consultant.ru/document/cons_doc_LAW_28399/
4. Синица А.Л. Труд по уходу за детьми дошкольного возраста: сочетание домашней и общественной форм // Дисс. на соискании уч. ст. к.э.н. по специальности Экономика и управление народным хозяйством (экономика труда). – М.: Научный центр проблем социального развития ОАО «Всероссийский центр уровня жизни», 2011. – 188 с.
5. Хуснутдинова Г.Ф., Воробьев Е.М. Женщины с детьми на рынке труда: мотивация и приоритетные сферы занятости // Современные проблемы науки и образования, 2015. – № 1-1. – Электронный ресурс. – URL: https://science-education.ru/ru/article/view?id=19176 (дата обращения: 30.03.2019).
6. Becker G.A. Theory of Allocation of Time // Economic Journal, 1965. – № 75 (299). – P. 493-517.
7. Booth A.L., Ours J.C., van. Hours of Work and Gender Identityç Does Part'Time Work Make the Family Happier? // Economica, 2009. – № 76 (301). – P. 215-236.
8. Doiron D., Kalb G. Demands for Child Care and Household Labor Supply in Australia // The Economic Record, 2005. – № 81 (254). – P. 176-196.
9. Gronau R. Leisure, Home Production, and Work – the Theory of the Allocation of Time Revisited // Journal Political Economy, 1977. – № 85 (6). – P. 1099-1123.

Работа выполнена при финансовой поддержке РФФИ, проект №18-010-00686.

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ЦИФРОВОЙ ЭКОНОМИКИ И ИХ ВЛИЯНИЕ НА СФЕРУ ОБРАЗОВАНИЯ В РОССИИ

Плоткин Александр Сергеевич
техник по защите информации ООО Русское Техническое Общество

Аннотация: *В статье рассматривается влияние цифровой экономики на сферу образования, в частности на вузы РФ. Выявление перспективных направлений развитие образовательного процесса.*

Ключевые слова: *информационная безопасность, цифровые технологии, цифровая экономика, развитие человеческого капитала.*

Abstract: *The article discusses the impact of the digital economy on the education sector, in particular, on the universities of the Russian Federation. Identify promising areas for the development of the educational process.*

Keywords: *information security, digital technologies, digital economy, human capital development.*

Введение. Цифровые технологии (далее - ЦТ) уже давно стали использоваться во всех сферах жизни. Человек уже перестал замечать, как те или иные вещи попадают в повседневную жизнь и какое влияние они оказывают на него и на мир вокруг. Многие услуги, для получения которых раньше приходилось идти в узко специализированные учреждения, сейчас доступны удаленно или в едином месте. Примером таких услуг служат различные электронные сервисы для граждан, такие как: ГосУслуги; МосРу; электронные дневники для образовательных учреждений и др.

Такие процессы происходят не только в сфере оказания услуг, но и в сфере образования. Данная сфера является наиболее важной, т.к. практическая реализация цифровых технологий может дать огромный скачок в развитии для всей экономики РФ. В частности, можно выделить, что именно воспитание подрастающего поколения с внедрением цифровых технологий в процесс обучения подготовит их к жизни в условиях цифровой экономики.

Цель исследования: изучить современные тенденции цифровой экономики и их влияние на сферу образования в России.

Задачи исследования:

- Проанализировать уровень развития цифровых технологий в мире.
- Определить основные факторы, влияющие на развитие цифровых технологий.
- Выделить тенденции в цифровых технологиях и основные направления развития.
- Разработать возможные пути цифровизации образовательных процессов в вузах РФ.

Многие развитые страны уже приняли подобное направление развития. Наиболее выделяющимися можно назвать: Норвегию, Швецию, Швейцарию, Данию, Финляндию, Сингапур, Южная Корею, Великобританию, Гонконг, США. Это показано на рисунке 1:

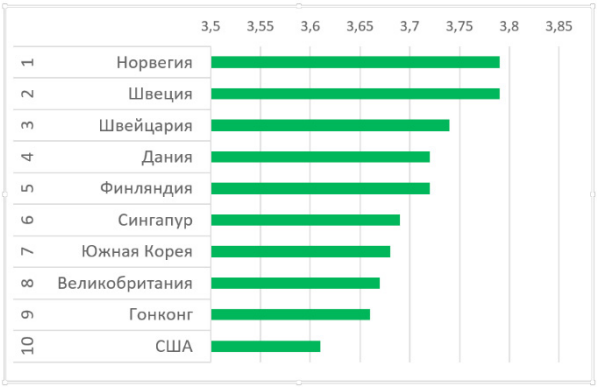


Рисунок 1. Digital Evolution Index (индекс цифровизации стран в 2018 году)

Сегодня более половины населения земного шара пользуется интернетом. Результаты исследования показывают конкурентоспособность и потенциал развития цифровой экономики в 60 странах.

С помощью рейтинга Digital Evolution Index 2018 оценивается каждое государство по 170 специально подобранным параметрам. Результаты данной оценки выделяют 4 основных фактора, с помощью которых можно определить темпы цифровизации страны (рисунок 2).

Данный рейтинг также показывает состояние и скорость развития ЦТ. Все страны делятся на 4 группы: замедляющие темпы роста (жёлтые), перспективные (зелёные), лидирующие (Фиолетовые) и проблемные (красные). Эти группы представлено на рисунке 3.

Россия по данному рейтингу является одной из наиболее перспективных стран для развития цифровых технологий. На данный момент в России общий

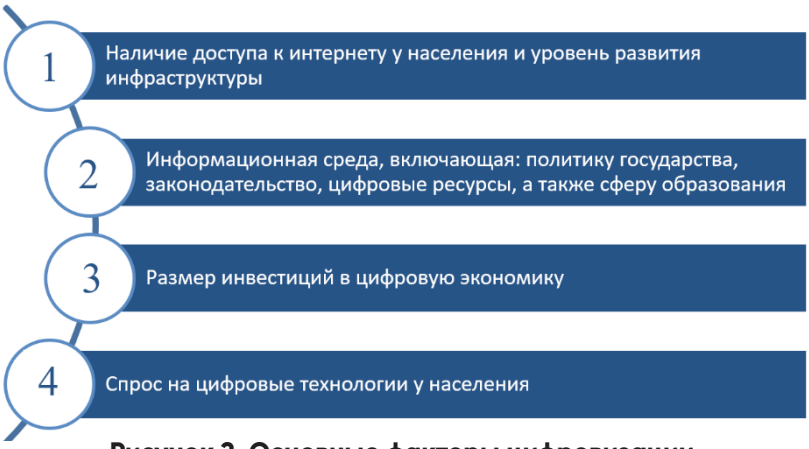


Рисунок 2. Основные факторы цифровизации

уровень цифровизации довольно низок, но при этом она показывает стабильные темпы роста цифровых технологий, поэтому она стала привлекательна для многих иностранных инвесторов. [4]

В РФ уже массово внедряются автоматизированные системы управления вузом. Они выполняют функции анализа и корректировки состояния других частей информационного пространства вузов (в частности, выполняют качественный и количественный анализ хода образовательных процессов). По результатам проведенного анализа удастся организовывать образовательные процессы на более высоком уровне. За счет собранной статистики и полученного анализа, администрация высших учебных заведений может объективно оценить, где требуется внедрение инноваций в процесс обучения. [1]

Для сопровождения и поддержки автоматизированной системы управления вуза требуются высококвалифицированные специалисты, следовательно, образовательные учреждения и стремятся получить таких специалистов. Намного эффективнее для вузов готовить их у себя, чем нанимать со стороны. Именно поэтому главной тенденцией в образовательных учреждениях становится развитие человеческого капитала, который есть совокупность знаний, умений и навыков, используемых для удовлетворения потребностей человека, как специалиста, так и общества в целом. На рисунке 4 можно увидеть, как повлияла данная тенденция на привлечение к работе в вузах молодых специалистов, только-только окончивших данные заведения.

Предполагается, что в недалеком будущем население будет обладать ключевыми универсальными компетенциями (умение критически мыслить, эффективно работать в команде и взаимодействовать с другими людьми) и высоким уровнем цифровой грамотности, а система образования будет отвечать потребностям цифровой экономики. Для развития человеческого капитала необходимо начинать прививать навыки и знания в области цифровых технологий ещё с раннего возраста, когда человек обучается в школе. А именно следует:

- обеспечить повсеместное внедрение основ программирования в начальном образовании;
- обеспечить обновление содержание пред-

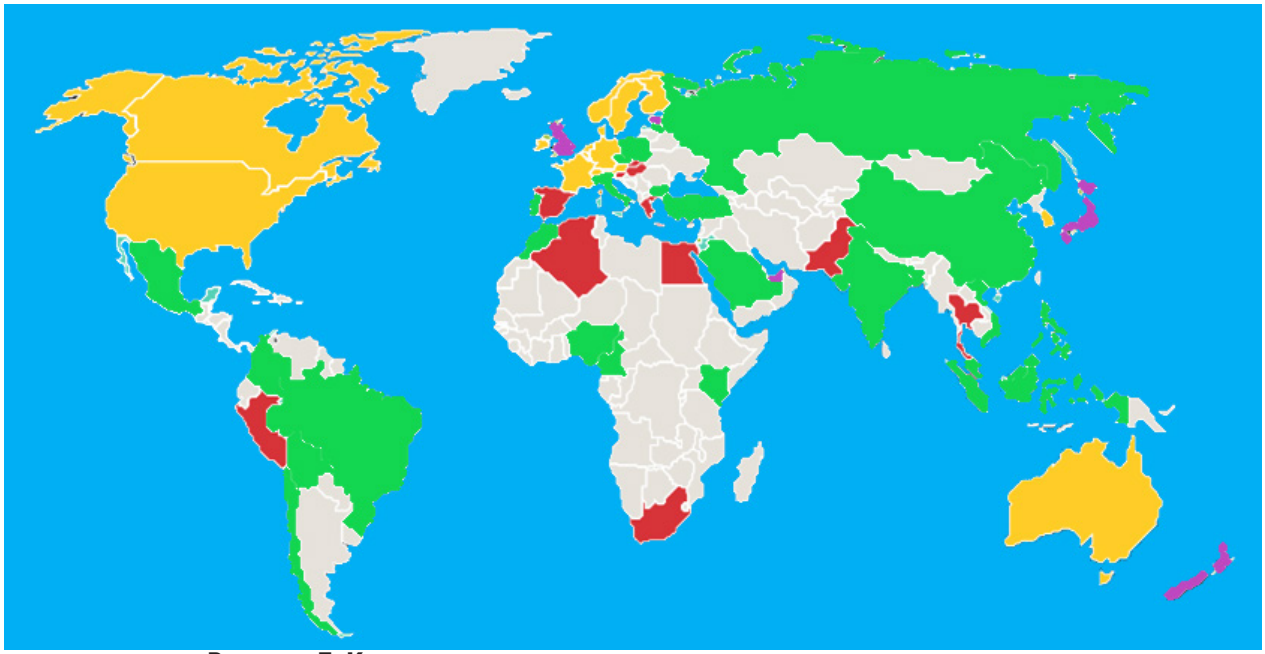


Рисунок 3. Карта мира, с распределенными по группам, странами

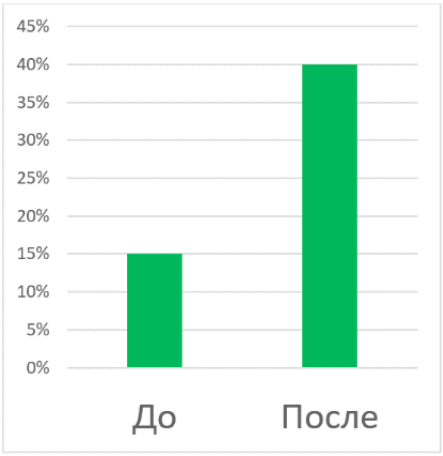


Рисунок 4. Диаграмма разницы до тенденции ЦТ и после

мета «Информатика»;
- обеспечить цифровизацию учебного процесса через предоставление доступа школьных учебных программ онлайн, с учетом развития дистанционного обучения.

Необходимо также улучшить и актуализировать обучение в высших учебных заведениях, путем внедрения новых учебных программ и специальностей, которые будут актуальны и в будущем. В частности, предлагается:
- актуализация учебных программ по требованиям рынка труда всех специальностей;
- развитие дистанционного образования;
- открытие ИКТ кафедр ВУЗов на базе производства;
- увеличение кол-ва государственных грантов по специальности ИКТ. [2]

После достижения положительных результатов ни в коем случае нельзя останавливаться. Нужно обеспечить непрерывное обучение и получение новых и актуальных навыков. Можно выделить следующие направления развития цифровой экономики в России:
- Создание и совершенствование регулирующих законов и правовых основ для благоприятного развития современных технологий;
- Обновление и совершенствование образовательных процессов, которые обеспечат цифровую экономику специалистами;
- Повышение защищенности отдельных граждан и государства от информационных угроз;
- Развитие сетевых технологий, центров обработки данных и технологий связи. [3, 5]

Вывод. Проанализировав проведённую исследовательскую работу можно сделать вывод, что существует зависимость между тенденциями в образовательных процессах и тенденциями в ЦТ. Уровень ЦТ в мире постоянно растёт, наиболее активно на это влияют инвестиции и цифровая грамотность, а также заинтересованность правительства в развитии ЦТ. Следует отметить, что такая тенденция как развитие человеческого капитала непосредственно влияет на сферу образования и на развитие ЦТ в целом. В таком случает необходимо активно развивать процесс и корректировать внедрение поддерживающих данные тенденции информационно-коммуникационных и образовательных технологий. За счет роста качества системы образования РФ и подготавливаемых ей специалистов, возможно, удастся обеспечить развитие экономики всей страны на основе построения высокотехнологичного и образованного общества.

Список литературы:

1. К. В. Пителинский, А. Ю. Хачатрян / Интегрированная система безопасности университетского комплекса - особенности построения и эксплуатации // Вопросы защиты информации. - 2010. - N 3. - С. 36-41. - Библиогр.: с. 41
2. Человеческий капитал. В сети интернет. URL: https://ru.wikipedia.org/wiki/Человеческий_капитал
3. Российское образование в эпоху «цифровой экономики» требует реформы. В сети интернет. URL: https://www.pnp.ru/social/rossiyskoe-obrazovanie-v-epokhu-cifrovoy-ekonomiki-trebuet-reformy.html
4. ТОП 10 стран с наиболее развитой цифровой экономикой. В сети интернет. URL: http://web-payment.ru/article/250/top-10-cifrovaya-/
5. Экономика Россия 24. В сети интернет. URL: https://data-economy.ru/

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ СОЗДАНИЯ ИНТЕРНЕТ-МАГАЗИНА

Карягина Татьяна Васильевна
кандидат технических наук, доцент кафедры информатики и прикладной математики, факультет информационных технологий, Российский государственный социальный университет, г. Москва

Пронькина Татьяна Васильевна
кандидат физико-математических наук, доцент института цифровой экономики Югорский государственный университет,
г. Ханты-Мансийск

Аннотация: *В статье описываются основные этапы создания интернет-магазина, а именно, рассматриваются необходимые теоретические аспекты создания платформы, на которой будет располагаться, и функционировать интернет-магазин.*

Ключевые слова: *интернет-магазин, сайт, хостинг, база данных, домен, контент.*

Abstract: *the article describes the main stages of creating an online store, namely, the necessary theoretical aspects of creating a platform on which the online store will be located and function.*

Keywords: *online store, website, hosting, database, domain, content.*

Введение. В настоящее время функциональность онлайн сервисов и платформ растет с развитием технологий, что позволяет организациям оптимизировать и автоматизировать производственный, управленческий и другие процессы. Общие тренды глобализации и интеграции в большинстве сфер человеческой деятельности происходят во многом благодаря Интернету и, в том числе, позволяют значительно ускорять развитие технологий сетевых компьютерных коммуникаций, которые появились как синтез самостоятельных, появившихся не в одно время и создававшихся с разными целями, однако взаимосвязанных по контенту компонентов (компьютерные технологии, сетевая архитектура) [5].

Основные этапы создания интернет-магазина

Чтобы начать разрабатывать новый интернет-магазин, необходимо выбрать хостинг и зарегистрировать доменное имя. Хостинг – это услуга, которая предоставляет место на сервере, постоянно функционирует в сети Интернет и служит для размещения и хранения файлов сайта. Сервер может находиться в любой стране и любом городе. Они могут обладать различными характеристиками, в зависимости от объема и мощности пространства диска для размещения на нем файлов. Существует четыре вида хостинга [4]:

виртуальный хостинг;

- виртуальный выделенный сервер;
- выделенный сервер;
- коллокация.

Виртуальный хостинг, т.е. когда на физическом сервере выделяется только определенное количество вычислительной мощности и пространства на диске, в соответствии с тарифом, который был приобретен у компании, предоставившей услуги хостинга. Самый дешевый вид и распространенный, он подходит для простых веб-сайтов и начинающих разработчиков.

Виртуальный выделенный сервер – это специальное программное обеспечение, которое эмулирует полноценный выделенный сервер внутри физического. Он использует часть физического сервера, но имеет все необходимое для полного управления и настройки функционала. Больше всего такой вид подходит для профессиональных сайтов, которые испытывают большую нагрузку и требуют сложных вычислительных процессов. Обычно на этот вид хостинга переходят, когда сайт начинает развиваться и ему начинает не хватать характеристик виртуального хостинга.

Выделенный сервер – это физический сервер с необходимой конфигурацией технических характеристик. Следует отметить, что это полноценный компьютер. Данный вид чаще всего используют крупные IT-проекты.

В случае коллокации происходит размещение собственного оборудования в дата-центре хостинг-провайдера для создания сервера. Это

подразумевает оплату аренды помещения и поддержания работоспособности оборудования.

Следующим этапом при создании сайта является регистрация доменного имени (DNS – Domain Name System). Далее рассмотрим определение и виды DNS.

DNS (Domain Name System) – это адрес интернет-пространства (сайта), по которому пользователь находит его в сети Интернет [3].

Доменное имя состоит из нескольких частей, которые также называют уровнями домена. Каждый уровень домена несет в себе определенную функцию.

Первый уровень относится к территориальной принадлежности домена (.ru – Россия, .us – США, .gb – Великобритания, .ua – Украина и др.) или к типам организаций (.com – коммерческие сайты, .edu – образовательные, .gov – правительственные и др.). Первоначальной причиной использования сокращений принадлежности доменного имени к определенной сфере деятельности или местонахождению сайта было удобство пользователя. С течением времени, такое определение принадлежности стало трудновыполнимым ввиду того, что создатели сайтов начали использовать его некорректно, вне контекста принадлежности к чему-либо.

Второй уровень, имя сайта, служит идентификатором уникальности сайта. Домен третьего уровня предназначен для создания разделов или дополнений к основному сайту. Пользователь может создать любое количество доменов этого уровня.

После регистрации и оплаты хостинг услуг, следует зарегистрировать доменное имя, которое оплачивается отдельно.

Выбрав свободный домен, нужно пройти обязательную регистрацию. Для этого необходимо будет указать «Тип персоны», что означает выбор между физическим лицом или юридическим. Индивидуальный предприниматель в данном случае будет входить в категорию физических лиц. Далее пользователю предоставят возможность указать страну, заполнить паспортные и контактные данные. При регистрации юридического лица нужно будет заполнить дополнительные пункты, раскрывающие регистрационные данные компании. Также обязательно указывается согласие на установку «Private Person», таким образом, выполняется закон «О персональных данных». При этом указанные ФИО не будут отображаться при проверке домена по общедоступной базе WHOIS. Одобрение регистрации доменного имени происходит в течение суток.

Следующим шагом, является создание базы данных, для управления которой используется MySQL – свободная реляционная система управления базами данных [6]. В административной панели хостинга пользователю нужно зайти во вкладку MySQL. Этот раздел предназначен для создания базы данных под управлением MySQL. Далее необходимо будет придумать имя базы и пароль, ввести их в специальное окно и нажать кнопку «Добавить».

Для того чтобы создать сайт, не имея при этом глубоких профессиональных знаний и навыков программирования, можно использовать CMS. CMS (от англ. Content Management System) – система управления содержимым (контентом) – информационная система или компьютерная программа, которая используется для организации, управлению и редактированию содержимого сайта [2].

Далее проанализируем наиболее лучшие системы управления контентом. Критерии отбора заключались в возможностях, которые может предоставить CMS, в степени удобства административной панели, грамотной работе системы техподдержки, а также, в наличии бесплатной лицензии. Аналитический портал рынка веб-разработок «CMSmagazine» предоставил рейтинг CMS разработок, состоящий, на данный момент, почти из 1000 различных CMS, 500 из которых предназначены для интернет-магазина. В данной работе произведен отбор CMS по предоставляемым порталом характеристикам, а именно, отобраны бесплатные типы CMS, по типу сайта выбран «Интернет-магазин». Получившийся рейтинг ранжирован по статистике «Количество работ». По итогам ранжирования, первые пять позиций были заняты следующими CMS [1]:

- OpenCart,
- Joomla,
- MODX,
- WordPress,
- Drupal.

Далее рассмотрим вышеописанные системы

OpenCart – одна из самых простых в управлении систем, административная панель которой интуитивно понятна. Она не требует больших мощностей, что позволяет использовать виртуальный хостинг. Большое русскоязычное сообщество, на форуме которого можно найти решения множества проблем, а также задать свой вопрос также является огромным преимуществом для неопытного пользователя. Широкий выбор модулей, как платных, так и бесплатных позволяет использовать множество возможностей для оптимизации работы сайта. В системе есть открытый код, позволяющий настроить интернет-магазин под свои нужды и потребности. Дополнительный функционал позволяет создавать скидки, купоны, акции, группы пользователей и т.п. В программе есть и свои минусы, одним из которых является ограниченные возможности системы. При большом количестве наименований товаров система начнет тормозить. Часто новые версии CMS несовместимы со старыми модулями, а для автоматизации систем нужно использовать платные версии. Таким образом, эта система подходит для начинающих разработчиков, которые создают небольшие интернет-магазины.

Система Joomla имеет множество плагинов для расширения своего функционала и большое количество шаблонов для настройки сайта под разные нужды. Эта CMS позволяет настроить оптимизацию сайта с помощью мета-данных и расширений. Однако большое количество дополнений увеличивает уязвимость, поэтому необходимо следить

за всеми обновлениями и правильной работой системы. Это нагружает систему, что может привести к заторможенной работе. Данная CMS больше подходит для информационных сайтов и страниц-визиток.

В системе MODx многие положительные черты схожи с OpenCart: такая же простая и понятная панель администратора, хороший модульный функционал SEO, система не нуждается в больших требованиях к хостингу. Однако большим минусом оказалось маленькое русскоязычное сообщество. Поиск решения проблем становится проблематичным. Недостаток – это малое количество шаблонов. Можно настроить для него CSS – шаблоны, но начинающему разработчику будет сложно это осуществить. Такая система подойдет для опытного web-разработчика.

WordPress – это очень простая и удобная система, она имеет плагины, модифицирующие сайт в интернет-магазин. Но большую нагрузку она не выдержит, а расширения будут ее только увеличивать. Данная CMS больше подходит для информационных сайтов, блогов и сайтов-визиток.

Drupal – хорошая система с большим сообществом и технической поддержкой. В ней есть около 30000 бесплатных расширений, увеличивающих функционал системы. Но в отличие от других систем, она имеет сложный интерфейс и этому сопутствует долгий процесс обучения. Еще один недостаток – это периодическое возникновение критической уязвимости. Таким образом, данная система не подойдет для начинающих специалистов.

Заключение.

В данной работе рассмотрены представленные системы (OpenCart, Joomla, MODX, WordPress, Drupal), в которых дано детальное описание преимуществ и недостатков, а также теоретические аспекты создания платформы, на которой будет располагаться, и функционировать интернет-магазин.

Список литературы:

1. «Рейтинг CMS для интернет-магазина» источник url: http://www.cmsmagazine.ru/catalogue/shop/?ctl=2
2. Бабаев А. Создание сайтов. М.: Питер, 2014. – 304 с.
3. Каплунов Д. Маркетинг и рок-н-ролл. Книга-муза для покорения клиентов в интернете. М.: Манн, 2018. – 384 с.
4. Карминский А.М. Информатизация бизнеса. Москва. 2003. – 620 с.
5. Карягина Т.В., Лебедева М.В., Фетисов В.А. Оптимальные портфельные решения в условиях глобализации // Инновации и инвестиции. 2015. №7. – С.91-95.
6. Карягина Т.В., Левкова Т.В., Подзорова М.И. Аудит интернет-магазина и факторы повышения его конверсии // Современная экономика: проблемы и решения. 2015. № 5 (65). – С. 42-52.

РАЗДЕЛ IV. ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ФИЗИЧЕСКОЙ КУЛЬТУРЫ, СПОРТА И ТУРИЗМА

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ТУРИЗМЕ И ГОСТИНИЧНОМ БИЗНЕСЕ

Седенков Сергей Евгеньевич
Преподаватель кафедры Туризма и гостиничного дела, ведущий тренер М ГФ Киокушинкай каратэ-до клуб GAMBARU DOJO. Российский государственный университет физической культуры, спорта, молодежи и туризма. Москва, Россия

Аннотация: *В статье проанализировано использование информацион-ных технологии в туризме и гостиничном бизнесе. Рассмотрена классифика-ция информационных технологий и влияние их на развитие туризма и гости-ничного дела.*

Abstract: *The article analyzes the use of information technology in tourism and hotel business. The classification of information technologies and their im-pact on the development of tourism and hospitality is considered.*

Ключевые слова: *Туризм, гостиничный бизнес, экономика, информа-ционные технологии.*

Keywords: *Tourism, hotel business, economy, information technology.*

Введение. Без преувеличения можно сказать, что в настоящее время информационные технологии играют важную роль в жизни, образовании, экономике. Создаются все новые и новые технологии, благодаря которым наша жизнь становится проще и комфортней. Вследствие появления телефонов или компьютеров, мы можем связаться с кем нужно и в любой момент. Информационные технологии позволяют автоматизировать многие процессы, например, оформление заказов, ведение учета, контроль персонала, подготовка отчетов, тем самым повышая качество работы и сокращая время на произведение действия.

Информационные технологии, развиваясь, дают толчок к развитию перевозок пассажиров, облегчает и улучшает процесс связи между туристскими предприятиями. Используя технологию онлайн бронирования, можно получить доступ к услугам с минимальными затратами времени, к примеру, на покупки билетов на самолет, бронирование гостиницы или же выбор тура.

Цели исследования – изучить влияние информационных технологий на развитие туризма и гостиничного дела.

Современные компьютерные технологии активно внедряются в сферу туристского и гостиничного бизнеса, и их применение становится неотъемлемым условием повышения конкурентоспособности любого туристского предприятия. Индустрия туризма позволяет использовать все многообразие компьютерных технологий, начиная от специализированных программных продуктов управления отдельной туристской фирмой до применения глобальных компьютерных сетей. На сегодняшний день в туризме используется достаточно много новейших компьютерных технологий, например, глобальные компьютерные системы резервирования, интегрированные коммуникационные сети, системы мультимедиа, Smart Cards, информационные системы менеджмента и др. Перечисленные выше информационные технологии используются с разной степенью активности и имеют неодинаковое распространение. Различается также степень их влияния на развитие туристской индустрии[1].

Влияние информационных технологий на туризм ощущается на разных стадиях создания и продвижения турпродукта.

Компьютерные системы резервирования CRS (Computer Reservation System), появившиеся в середине 60-х гг. XX в., позволили ускорить процесс резервирования авиабилетов и осуществить его в режиме реального времени. В результате этого повысилось качество сервисных услуг за счет уменьшения времени обслуживания клиентов, увеличения объемов и разнообразия предлагаемых услуг и т.д., а также появились возможности обеспечения оптимизации загрузки авиалайнеров, реализации стратегии гибкого ценообразования, применения новых управленческих методов и т.д. Высокая надежность и удобство этих систем резервирования способствовали их быстрому и широкому распространению. В настоящее время 98 % зарубежных предприятий сферы туризма используют системы бронирования. На российском рынке представлены в основном такие системы глобального резервирования, как Amadeus, Galileo Worldspan.

Одним из основных направлений применения

информационных технологий в туризме является внедрение мультимедийных технологий, в частности справочников и каталогов. В настоящее время туристские справочники и каталоги выпускаются в книжном исполнении, на видеокассетах, на лазерных дисках CD-ROM, в сети Интернет. Электронные каталоги позволяют виртуально путешествовать по предлагаемым маршрутам, просмотреть эти маршруты в активном режиме, получить информацию о стране, объектах по трассе маршрута, данные о гостиницах, кемпингах, мотелях и других средствах размещения, ознакомиться с системой льгот и скидок, а также законодательством в сфере туризма. Кроме того, в этих каталогах обычно приводятся информация о правилах оформления туристских документов, туристские формальности, модели поведения туриста в экстремальных ситуациях и т.д. Клиент может спланировать программу тура, выбрать его по заданным оптимальным параметрам (цена, система льгот, система транспорта, сезон и др.).

Использование мультимедийных технологий оперативно предоставляет потенциальному клиенту информацию о любом интересующем его туре и тем самым позволяет быстро и безошибочно выбрать подходящий турпродукт. При этом туроператор (турагент) имеет возможность при необходимости внести изменения в данный тур или сформировать новый эксклюзивный тур, произвести бронирование мест и продать туристу созданную в оперативном режиме туристскую услугу.

Разработки специализированных программных продуктов для туристского бизнеса в настоящее время ведут несколько российских фирм: «Мегатек» (программа «Мастер-Тур»), «Арим-Софт» (программы TurWin, «Чартер», «Овир»), «Само-Софт» (программа «Само-Тур»), «Туристские технологии» (программа комплексной автоматизации «Туристский офис»), «Интур-Софт» (программа «Интур-Софт»), ANT-Group (система ANT-Group), «Рек-Софт» (комплекс «Эдельвейс», «Барсум», «Реконлайн») и др.

Наряду с автоматизацией туристских фирм ведется аналогичная разработка программ автоматизации деятельности гостиниц, ресторанов и других предприятий туристского бизнеса. Применение информационных систем в этой области приводит к существенным изменениям в менеджменте, а также повышает качество обслуживания.

В гостиничном бизнесе информационные технологии используются уже несколько лет. При помощи ИТ гостиницы организуют системы учета клиентов: базы данных, которые позволяют вести учет всех гостиничных номеров и клиентов. Большинство отелей имеют свой сайт, через который клиент может заранее зарезервировать номер и даже выбрать развлекательные и экскурсионные программы на свой вкус. Но мало кто решился перевести использование ИТ технологий в гостиничном бизнесе на новый уровень. Использовать ИТ для предоставления максимума информационных технологий для клиентов (рисунок 1).

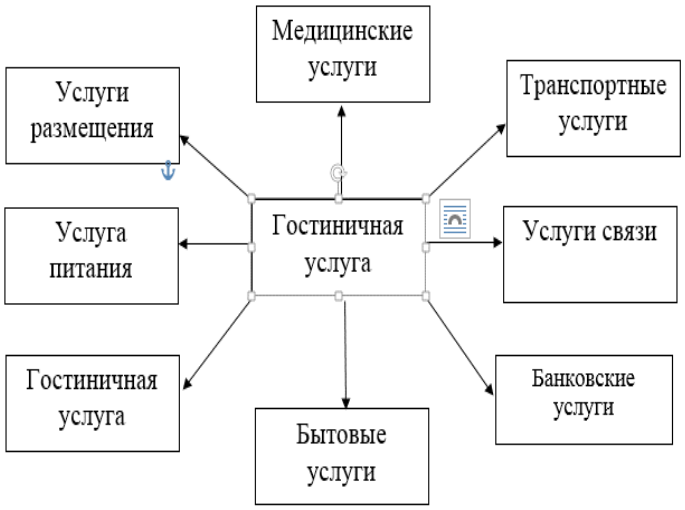


Рис. 1. Услуги, используемые гостиничным бизнесом. [Источник: составлено автором]

Классификация информационных технологий

Современная индустрия туризма, в последние годы, существенно изменилась. Успешное функционирование фирмы на рынке практические невозможно без использования информационных технологий. Специфика технологии разработки и реализации турпродукта требует таких систем, которые в кратчайшие сроки предоставляли бы сведения о доступности транспортных средств и возможностях размещения туристов, обеспечивали бы быстрое резервирование и бронирование мест, а также автоматизацию решения вспомогательных задач при предоставлении туристских услуг (параллельное оформление таких документов, как билеты, счета и путеводители, обеспечение расчетной и справочной информацией и др.). Это достижимо при условии широкого использования в туризме современных компьютерных технологий обработки и передачи информации[2].

Индустрия туризма настолько многолика и многогранна, что требует применения самых разнообразных информационных технологий, начиная от разработки специализированных программных средств, обеспечивающих автоматизацию работы отдельной туристской фирмы или отеля, до использования глобальных компьютерных сетей. Информационные технологии, используемые в туризме, приведены в рисунке 2.

Выводы. В работе была рассмотрена классификация информационных технологий, применяемая в туризме и гостиничном деле. Исходя из этого можно сделать выводы, что работа турагентства или же гостиницы, в наше время, практический не представляется возможной без их помощи. Так же, с появлением информационных технологий, клиенты могут без труда сами найти себе подходящий тур, подобрать авиабилет, выбрать для себя лучшую гостиницу и связаться с представителями. Для автоматизации всего этого были созданы программы (классификация представлена выше), которые помогают как работникам туристского бизнеса,

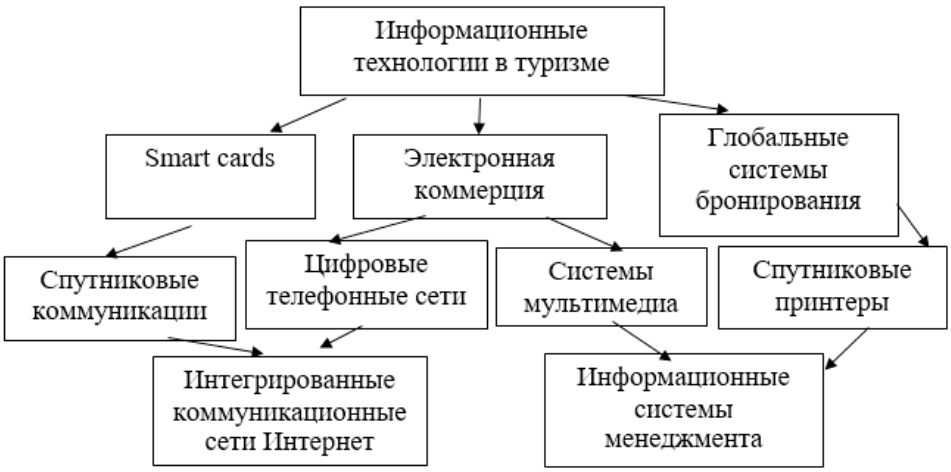


Рис 2. Использование информационных технологий в туризме. [Источник: составлено автором]

так и их клиентам. Новая технология вносит также большой вклад в метод работы гостиниц. Основные области применения компьютеров в гостиницах расширяются от их признанной роли в системах бронирования до процедур администрирования и ведения учетных записей гостей, до функций гостиниц по закупкам, контролю над запасами и общему бухгалтерскому учету, а также до других аспектов операций гостиницы и образуют комплексные информационные системы управления, которые дают возможность тесной координации и мониторинга всего бизнеса. Существенным результатом развития за последние годы явился быстрый рост систем компьютерного резервирования (CRS), глобальных систем распространения (GDS) и систем центрального резервирования. Интерактивные системы электронных данных, разработанные вначале авиакомпаниями, обеспечивают прямой доступ через оконечные устройства не только к компьютерам авиалиний, но также к компьютерам гостиниц и других операторов для выяснения наличия продукции, резервирования и выписки билетов или подтверждений. Лидирующие гостиничные консорциумы, перечисленные в приложении G, используют возможность новой технологии для поиска рынков сбыта гостиничных услуг своих участников по всему миру. Глобальные системы распространения дают эти консорциумам возможность обновлять информацию о наличии свободных номеров и ценах.

Список литературы

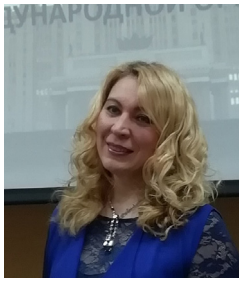
1. Биржаков М.Б. Введение в туризм. Учебник. М.: СПб: Герда, 2006
2. Лучко О.Н., Маренко В.А. Туристские услуги как фактор снижения когнитивного диссонанса личности//Индустрия туризма: возможности, приоритеты, проблемы и перспективы. 2015. № 8-1. С. 109-112.

РАЗДЕЛ V. МОЛОДЫЕ УЧЕНЫЕ – ПОИСК САМООПРЕДЕЛЕНИЯ

СТАТИСТИЧЕСКИЙ АНАЛИЗ ЭКОНОМЕТРИЧЕСКОЙ МОДЕЛИ И ПОСТРОЕНИЕ ТЕСТОВОГО ПРОГНОЗА

Емельянова Анна Александровна
Студентка 2-го курса факультета ИТ, по специальности прикладная математика и информатика, (г. Железногорск)

Зиновкин Андрей Витальевич
Студент 2-го курса факультета ИТ, по специальности прикладная математика и информатика, (г. Санкт-Петербург)



Бритвина Валентина Валентиновна
Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета, Доцент УИТС СТАНКИН

Аннотация: *В статье проведен анализ эконометрической модели применение которой определит перспективы развития малого и среднего бизнеса, основной акцент в исследовании сделан на общеизвестные факторы показатели деятельности. Построение уравнения регрессии на основании данных различных государств позволяет утверждать, что разработанная модель носит универсальный характер.*

Ключевые слова: *Эконометрическая модель, предприятия малого и среднего бизнеса, регрессия.*

Abstract: *The article analyzes the econometric model, the use of which will determine the prospects for the development of small and medium-sized businesses, the main emphasis in the study is made on the well-known factors of performance. The construction of the regression equation on the basis of data from different States suggests that the developed model is universal*

Keywords: *Econometric model, small and medium-sized businesses, regression, forecast., прогноз.*

Введение. Малые и средние предприятия играют важную роль в экономиках развитых и развивающихся стран. ВЕС малые и средние предприятия – это 99% всех компаний [1] и 85% всех рабочих мест [2]. Как отмечено в предисловии к докладу ОЭСР «Малые, средние, сильные. Тенденции в секторе МСП и условия ведения бизнеса» [3], значительная роль малых и средних предприятий в экономике стран стала еще более заметной после кризиса 2008–2009 гг., поскольку особенно негативное влияние кризиса коснулось именно этой группы предприятий.

Подчеркивают и выделяют значимость развития субъектов МСП в роли основного двигателя экономики как российские ученые (О. А. Блинов [4], В. Ю. Диденко, Н. И. Морозко [5], А. И. Орлов [6]), так и зарубежные (Ö. C. Bozkurk [7])

Проанализированы научные исследования, на основе которых определено отсутствие комплексных исследований, так как методы, используемые для крупных предприятий, для этого не всегда пригодны. Систематизированы подходы разных авторов к формированию регрессионных моделей, характеризующих влияние тех или иных факторов на деятельность организации. Выявлено, что в качестве результирующего показателя в исследованиях используются показатели количества предприятий малого и среднего бизнеса в странах. При этом главным недостатком большинства моделей является математический, а не

экономический подход к определению зависимых и независимых переменных. Модель построена с использованием данных о деятельности предприятий, работающих в восемнадцати странах.

Анализ эконометрической модели

Для построения модели были взяты данные о количестве предприятий среднего и малого бизнеса, уровню экономической свободы, ВНД, средней заработной платы, ВВП и уровню организованной преступности по 18 странам за 2017 год.

В итоге после исключения факторов получилась модель с только значимыми факторами. Она имеет линейный вид и выглядит следующим образом:

Гетероскедастичность проверим с помощью двух тестов: теста Уайта и теста Парка. Для теста Уайта составим вспомогательную регрессию и проанализируем её инструментом «Регрессия».

Таблица 1. Результаты инструмента Excel «Регрессия» для вспомогательной регрессии теста Уайта

ВЫВОД ИТОГОВ	
Регрессионная статистика	
Множест. R	0,74653964
R-квадрат	0,557321435
Нормир. R-квадрат	0,372872032
Станд. ошибка	4887819,56
Наблюдения	18

Дисперс. анализ

	df	SS	MS	F	Значим. F
Регрес-сия	5	3,609E+16	7,218E+15	3,0215	0,0540
Остаток	12	2,866E+16	2,389E+15		
Итого	17	6,476E+16			

Уравнение значимо по F-критерию, следовательно, тест Уайта показал гомоскедастичность остатков модели. Проведём дополнительно тест Парка. Построим несколько вспомогательных уравнений регрессии для каждого из факторов и проверим коэффициенты при них на статистическую значимость.

ttабл	2,13145	
X3:		
	-0,68939	22,63022
	0,802516	5,957257
tфактич	-0,85903	незначим
X4		
	0,147039	16,69706
	0,365159	2,104758
tфактич	0,402669	незначим

Рисунок 2. Проверка статистической значимости коэффициентов вспомогательной регрессии теста Парка

Каждый из коэффициентов оказался статистически не значим. Следовательно, тест Парка так же показал отсутствие гетероскедастичности. На основании результатов двух тестов можно заключить, что гетероскедастичности остатков построенной модели регрессии нет.

Автокорреляцию остатков проверим с помощью критерия Дарбина-Уотсона. Подсчитаем значение критерия Дарбина-Уотсона, и определим, в котором из интервалов он располагается.

d=	1,698142555	dl	1,16		
		du	1,39		
	du		4 - du		
	1,39	< d <	2,61	- автокорреляции нет	

Рисунок 3. Выявление автокорреляции остатков на основе критерия Дарбина-Уотсона

Как видно значение критерия равно 1,69814, и это значение попадает на интервал между и , следовательно автокорреляции нет.

Оценка точности уравнения

Множественный коэффициент корреляции равен 0,98611, что говорит о тесной связи факторов с результирующим признаком. Коэффициент детерминации равен 0,97241, то есть около 97 процентов вариации результирующего показателя объясняется уравнением регрессии, а около трёх процентов приходится на не учтенные в модели факторы.

Стандартная ошибка регрессии равна 10180,28. Сравнительно с данными это достаточно много, что говорит о пониженной точности прогнозов по построенному уравнению регрессии. Коэффициент детерминации достаточно высок, и в модели отсутствует гетероскедастичность остатков.

Тестовый прогноз

Проведем проверочный прогноз, используя полученное уравнение регрессии. В качестве данных возьмем среднюю заработную плату и показатель ВВП Польши за 2017 год. Данные для прогноза представлены на рисунке 4.

Данные для прогноза:			
Страна	y	x3	x4
Польша	72938	798	468

Рисунок 4. Данные для прогноза

Спрогнозируем по заданным показателям количество предприятий. Подставив их в уравнение регрессии получим 52057,96221. Рассчитаем доверительные интервалы, при уровне значимости 0,05 и проверим, попадёт ли в них реальное значение количества малых и средних предприятий в Польше за 2017.

В итоге получилось, что реальное значение попадает в доверительные интервалы.

Вывод. Уравнение регрессии было проанализировано, тесты Парка и Уайта показали отсутствие гетероскедастичности остатков построенной модели. С помощью критерия Дарбина-Уотсона проверили на отсутствие автокорреляции

остатков.

	Коэффициенты	
Y-пересечение	18696,0579	
x3	-7,286297212	
x4	83,71019121	
Стандартная ошибка	10180,28687	
tтабл(a = 0,05)	2,131449546	
Yпрогн.	52057,96221	
a = 0,05		
30359,19439	< Y <	73757
Польша	72938	

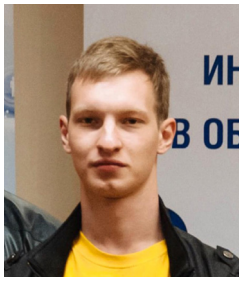
Рисунок 5. Доверительные интервалы для прогноза

Построение уравнения регрессии на основании данных различных государств позволяет утверждать, что разработанная модель носит универсальный характер. Однако из-за обобщения данных точность модели была снижена. Но при использовании представленной регрессионной модели и построении уравнения регрессии по данным стран Европы или экономико-политическое развитие которых схоже с общеевропейским, эта проблема будет нивелирована. Ценность полученной нами регрессионной модели заключается в том, что даже при высоком значении стандартной ошибки прогнозные значения входят в доверительный интервал. С помощью представленной модели был произведен прогноз на 2018 год для Польши. Это свидетельствует о практическом подтверждении применения данной модели для прогнозирования исследуемых экономических показателей. Поскольку целью исследования являлась разработка экономико-математической модели, применение которой определит перспективы развития малого и среднего бизнеса, основной акцент в исследовании сделан на общеизвестные факторы показатели деятельности. Таким образом, дальнейшим направлением исследования может являться анализ дополнительных переменных, отражающих влияние на деятельность предприятий. Включение данных переменных в модель позволит повысить качество модели в целом.

Список литературы:

1. Japan Bank for International Cooperation. Export Loans [Электронный ресурс]. URL: https://www.jbic.go.jp/en/support-menu/export.html
2. The Export-Import Bank of Korea. Hidden Champion Initiative [Электронный ресурс]. URL: https://www.koreaexim.go.kr/site/homepage/menu/viewMenu? Menuid = 002002002007001001
3. Agricultural Tariff Tracker [Электронный ресурс]. URL: https://apps.fas.usda. gov/ agtariff-tracker/Home/Search
4. Блинов А. О. Экологическое развитие малого предпринимательства // Стратегии бизнеса. 2015. № 3. С. 3–8.
5. Диденко В. Ю., Морозко Н. И. Оценка эффективности стратегического финансового управления организациями малого бизнеса // Экономика. Налоги. Право. 2015. № 2. С. 94–100.
6. Орлов А. И. О некоторых подходах к экономико-математическому моделированию малого бизнеса // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2015. № 108. С. 288–315.
7. Kalkan A., Bozkurk Ö.C. The choice and use of strategic planning tools and techniques in Turkish SMEs according to attitudes of executives // 9th International Strategic Management Conference. Procedia – Social and Behavioral Sciences. 2013. No. 99. Pp. 1016–1025.

АНАЛИЗ БЕЗОПАСНОСТИ БЕСПРОВОДНОЙ СЕТИ



Закревский Александр Сергеевич
Студент 4 курса, направление: «Информационная безопасность автоматизированных си-стем» Московского политехнического университета

Будылина Евгения Александровна
Кандидат физико-математических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета.

Аннотация: *В статье рассматриваются протоколы безопасности беспроводной сети, их ограничения и недостатки. Также рассмотрена атака с использованием ключа восстановления, и продемонстрирована его эффективность в уменьшении среднего числа пакетов перехвата на основе выбора векторов инициализации. Было проведено ряд сравнительных экспериментов по атакам только зашифрованным текстом, чтобы изучить эффективность такой техники и подчеркнуть возникшие трудности.*

Ключевые слова: *информационная безопасность, цифровые технологии, Wi-Fi, : WEP, WPA, WPA2, FMS, протоколы передачи данных.*

Abstract: *the article discusses wireless network security protocols, their limitations and disadvantages. An attack using a recovery key is also considered, and its effectiveness in reducing the average number of intercept packets based on the selection of initialization vectors is demonstrated. A number of comparative experiments on ciphertext-only attacks were conducted to examine the effectiveness of such a technique and highlight the difficulties encountered*

Keywords: *information security, digital technologies, Wi-Fi,: WEP, WPA, WPA2, FMS, data transfer protocols.*

Введение. В последние время наблюдается значительное увеличение развития беспроводных сетей; они становятся неотъемлемой частью Интернета и демонстрируют эффективность в управлении связью для ограниченных общедоступных локальных сетей и военных приложений. В основном это связано с их мобильностью и дешевыми решениями; тем не менее, они также подвержены нескольким атакам, связанным с целостностью данных, отказом в обслуживании и прослушиванием. На самом деле, беспроводные сети становятся важным инструментом связи благодаря своей гибкости, эффективности и низкой стоимости. С другой стороны, беспроводные сети имеют много ограничений в отношении традиционных сетей, таких как уменьшение объема данных и низкое энергопотребление [1,2]. Кроме того, беспроводные сети передают данные с помощью радиоволн, которые обычно чувствительны к прослушиванию; хотя необходимо сохранять данные, передаваемые через сетевые узлы, постоянно зашифрованными, чтобы предотвратить несанкционированный доступ к своему контенту. В беспроводных сетях управление связью осуществляется протоколами WEP, WPA и WPA2, разработанными для защиты связи. Однако и с учетом их ограничений решения для безопасности, предназначенные для таких сетей, становятся недостаточными для защиты от атак на секретные ключи. Целью данного исследования является описание вопросов, связанных с безопасностью в беспроводных сетях; Мы сосредоточены на протоколах WEP и WPA, которые все еще широко используются, но также не способны обеспечить защиту от различных угроз и уязвимостей, таких как атака FMS, которая основана на слабости вектора инициализации и требует около 4 миллионов пакетов для восстановления секретного ключа [3]. , Наш вклад заключается в том, чтобы найти лучший способ выбора, чтобы уменьшить среднее количество пакетов перехвата, необходимых для восстановления секретного ключа. Этот факт уменьшает время прослушивания при использовании пассивных атак. Итак, после введения в статье представлен краткий обзор существующих беспроводных протоколов, их особенностей и недостатков в разделах 2; Раздел 3 представляет справочную информа-

цию о предыдущих работах, связанных с угрозами и атаками [4]. Мы фокусируемся на производительности атаки FMS в разделе 4, затем следуют некоторые сравнительные эксперименты, основанные на статистическом анализе объема перехваченного трафика с целью выявления секретных ключей, после чего обсуждаются результаты и выводы.

Wi-Fi Протоколы: проводные соединения на основе стандарта IEEE 802.11 позволяют подключать ноутбуки, настольные компьютеры, КПК или любое устройство с широкополосным соединением на расстоянии нескольких сотен метров в открытой среде. Wired Equivalent Privacy (WEP), часть стандарта IEEE 802.11, создана в 1999 году и широко применяется на устройствах WLAN; он разработан для обеспечения конфиденциальности, аутентификации и целостности, аналогичных проводным сетям [5]. WEP основан на схеме шифрования RC4 и CRC-32 для обеспечения целостности данных и использует секретный ключ сегмента k длиной от 5 до 13 байтов. Чтобы создать зашифрованный текст C и его контрольную сумму ICV из открытого текста M, ключ k объединяется с вектором инициализации из 3 байтов в соответствии со следующей формулой (1):

$$C=M||ICV(M) \oplus RC4(K)||IV$$

где || обозначает оператор конкатенации, а $\oplus$ - побитовый исключающий оператор ИЛИ.

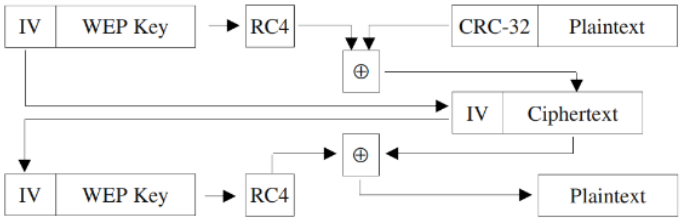


Рисунок 1. WEP процесс инкапсуляции

Вектор является краеугольным камнем безопасности WEP; он увеличивается для каждого испускаемого пакета, чтобы два последующих пакета не могли быть зашифрованы одним и тем же ключом. Это предполагает поддержание достойного уровня безопасности и предотвращение утечки информации [6]. WEP был задуман как первый инструмент безопасности сетей Wi-Fi. WEP призван быть относительно эффективным и реализуемым как в аппаратном, так и в программном обеспечении. Кроме того, испускаемые пакеты шифруются отдельно независимо друг от друга, что позволяет избежать повторной синхронизации при потере пакетов. Защищенный доступ Wi-Fi (WPA) является улучшенной версией стандарта 802.11i, разработанной Wi-Fi-Aliance в 2001 году [7]. Он основан на протоколе целостности временного ключа (TKIP), надежном алгоритме шифрования, построенном на основе WEP; это позволяет генерировать случайные ключи, которые отключают атаки на основе статистического анализа. WPA включает некоторые улучшенные свойства, такие как код целостности сообщения (MIC) и хэш-функция ключа, чтобы избежать атак. Рисунок 2 иллюстрирует процесс WPA-TKIP, где TK, DA, SA обозначает соотв. временный ключ, адреса отправителя и получателя и ||, оператор конкатенации.

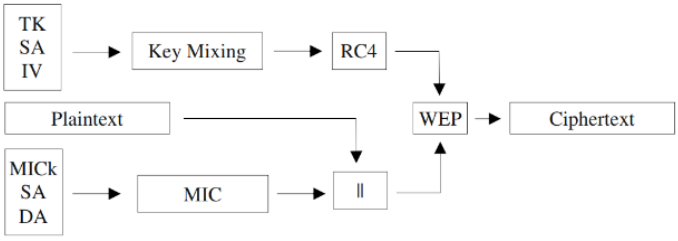


Рисунок 2. WPA процесс инкапсуляции

Обзор безопасности протоколов Wi-Fi: конфиденциальность и целостность данных являются наиболее важной проблемой в безопасности беспроводных сетей, особенно при обмене конфиденциальной информацией о промышленных, военных приложениях или распределении ключей. Защита WEP основана на структуре Rivest Cipher 4 (RC4), алгоритме потокового шифра, где открытый текст X-ored с последовательностью случайных байтов, сгенерированных алгоритмом планирования ключей (KSA) и алгоритмом псевдослучайной генерации (PRGA), части RC4, однако, доказано, что эти байты на самом деле не случайные, как они должны быть; они построены на длине ключа 64 бита, но на самом деле 40 бит фиксированы. Оставшиеся 24 бита предлагают всего 16 миллионов возможностей и, статистически, дают 50% шанс повторного использования IV после менее чем 5000 пакетов; однако, это может быть уязвимым для парадоксальной атаки на день рождения. Кроме того, в WEP используется один ключ, общий для всех узлов и точек доступа, и он не часто меняется. Основываясь на этих недостатках, WEP уязвим для нескольких ключевых типов атак, таких как DoS-атаки, захваты узлов, анализ трафика и т. д. Borison et al. представили некоторые недостатки в WEP, связанные со структурой RC4, которая состоит из инициализации и увеличения их на единицу для каждого использования [8]. А поскольку пространство клавиш сокращено, что дает высокую вероятность повторного использования потоков ключей; Слабость также была обнаружена Fluhrer et al. с использованием атаки FMS; идея заключалась в том, чтобы идентифицировать слабые клавиши, которые можно использовать для определения набора выходных битов; Результаты показали, что для восстановления секретного ключа достаточно 4 миллионов пакетов. Та же атака требует более 5 миллионов пакетов для восстановления секретного ключа в другой реализации, реализованной в. Подобно атаке FMS, атака Korek пытается выявить начальные биты ключей из блоков данных, сгенерированных алгоритмом PRGA; Результаты были получены методом грубой силы на наборе 1 миллион ключей. Несколько других атак, таких как атака Клейна , атака PTW , позволили раскрыть секретный ключ с 30–60 тысячами пакетов. VV атака использует случайные пакеты; Результаты показали, что для восстановления секретного ключа достаточно 32 тысяч

пакетов. Эти результаты были уменьшены до 24 тысяч Beck et al. Используя разные ключи для каждого зашифрованного пакета, успешные атаки на протоколы WPA и WPA2 кажутся редкими и сложными на практике. DoS, основанные на атаках, где они часто используются, пытаются насыщать целевой компьютер внешним трафиком, чтобы замедлить его; атаки заставляют систему перезагружаться; следовательно, он становится не в состоянии идентифицировать законные запросы [9]. Также является популярной атакой, она нацелена, в частности, на GTK, общий ключ для всех сетевых устройств, используемых для широковещательного трафика, который не может обнаружить подделку адресов и подделку данных. Этот ключ позволяет пользователю в сети осуществлять атаку, такую как DoS или спуфинг DNS, путем внедрения трафика из одной точки доступа в другие машины, связанные с той же самой точкой доступа. Этот акт продвигает машины-жертвы для пересылки трафика, предназначенного для точки доступа. Злоумышленник способен перехватывать все незашифрованные пакеты, не будучи обнаруженным точкой доступа. Аналогично, другие атаки были также выполнены на TKIP, BT-атака состоит в том, чтобы выполнить незначительные изменения в коротких пакетах ARP и DNS для восстановления открытого текста и потока ключей и, в свою очередь, перейти к атакам отравления DoS и ARP. Атака BT была улучшена атакой Ohigashi-Morii , которая сочеталась с атакой «человек посередине», чтобы сократить время выполнения. Таблица 1 иллюстрирует наиболее популярные атаки на протоколы WEP и WPA, где секретный ключ раскрывается по количеству упомянутых пакетов.

Обзор атаки FMS: секретный ключ k и вектор инициализации представляют собой основной недостаток протокола WEP; только 3 байта изменяются для каждого передаваемого пакета, в то время как 13 байтов k все еще статичны. Эти недостатки используются большинством атак против ключевых потоков. FMS, известная атака открытого текста, требует знания первого байта ключевого потока и большого количества векторов инициализации, чтобы иметь достаточно слабого, необходимого для успеха атаки. FMS основана на двух условиях:

а. На итерации i KSA, если мы достигли стадии, где x = Si , y = Si [x], x + y = Si [x] + Si [Si [y]] с 1<i<x<x+y; тогда вероятность 5% того, что ни один из элементов x, y и x + z не будет использоваться в последующих итерациях, и S [x] + S [S] может быть первым байтом, сгенерированным PRGA. Эта ситуация называется разрешенным состоянием.

б. В разрешенном состоянии показывает, что значение следующего байта ключа ключа k с вероятностью 5% будет равно $S(b)=S_{b+2}^{-1}[Out]-J_{b+2}-S_{b+2}[b+3]$, если S [1] <I и S [x] + S [S [1]] = I + b, где Out - первый выход PRGA; I, S, S-1 являются векторами состояния KSA для первых b итераций. При применении WEP мы предполагаем, что мы знаем первые байты секретного ключа k , .., k [a + 2]. Изначально мы имеем a = 0, поэтому известны только 3 байта. Исходя из этих соображений, FMS пытается смоделировать первые x итераций KSA, что позволяет определить перестановку Sx-1 и связанные с ней индексы ix-1 и jx-1. Следующее значение i также известно (ix = x), но следующее значение j зависит от следующего выбранного байта ключа. Байт случайного ключа имеет только 5% шансов быть верным; таким образом, можно определить следующий байт ключа среди нескольких байтов-кандидатов при их появлении, извлеченных из большого количества пакетов. Этот принцип может быть выбран при выборе всех следующих байтов ключа. Как это указывает, успех такой идеи зависит

Таблица 1. Сводка самых популярных атак восстановления секретных ключей

Protocol	Attack	Type	IV-search	Year	Packets (million)
WEP	FMS [10]	Statistical	Random	2001	4-6
	Korek [13]		Random	2004	0.1
			Brute-force		0.001-1
	PTW [15]		Random	2007	0.04
			Brute-force		1
	VV [16]		Random	2007	0.32
	Klein [14]	Key-recovery	Random	2008	0.25-0.6
	BT [17]		Aircraft-ng	2009	0.24
WPA	Dictionary attack	Key-recovery			
	Beck and Tews [19]	QoS		2009	
	Ohigashi-Morii [20]	Inject packets		2009	
	Hole196 [18]	Man-in-the-middle		2010	

от слабого пакета. Слабый пакет позволяет раскрыть информацию о ключевых байтах, он имеет особую форму (a + 3, 255, x), где a обозначает k-байт, который должен быть найден, а x не имеет значения. Эта форма обозначена высокой корреляцией между пакетом и выходом PRGA. Поскольку IV просты, слабые IV легко обнаружить. Другой вариант Weak-IV, называемый независимыми от ключа слабыми пакетами, предложенный с приведением к t = S3 [1] + S3 [S3 [1]] и используемый для угадывания k [t], где 3 t. Также Fluhrer & al. [предложил другой способ выбора: зависимые от ключа слабые приводят к SI [1] <I и SI [x] + SI [SI [1]] = I + b, где I, размер IV (= 3) и a, угаданный a-тый байт ключа.

Экспериментальное исследование: обзор реализации FMS-атаки на протоколы WEP. Цель эксперимента - проанализировать эффективность такой атаки в реальной среде Wi-Fi, ее стоимость и, если возможно, внести свой вклад в ее улучшение. Эксперименты проводились на 3,2 ГГц процессоре; среда включает пакет aircrack-ng в системе Linux; нам также необходимо установить беспроводную карту в режиме монитора. Для сбора данных мы используем инструмент airdump-ng, переключаемый на определенные пакеты AP из одного канала. Мы использовали совместимый сетевой интерфейс, который позволяет генерировать и вводить пакеты для увеличения трафика. Захваченные пакеты были разделены на три файла в соответствии с их особенностями: специфическая форма, зависимость от ключа слабая и независимая от ключа слабая. Кроме того, все захваченные пакеты были сохранены в другом файле, который использовался для исчерпывающего поискового теста [10]. Наконец, мы приступаем к атаке, которая выглядит типовой: для каждого байта ключа мы выбираем файл, каждый пакет соединяется с секретным ключом и переходим к первым трем итерациям алгоритма KSA. Затем мы можем искать каждый байт ключа, который проверял разрешенное условие, используя aircrack-ng. Гистограмма на следующем рисунке показывает изменение времени процессора для каждой категории.

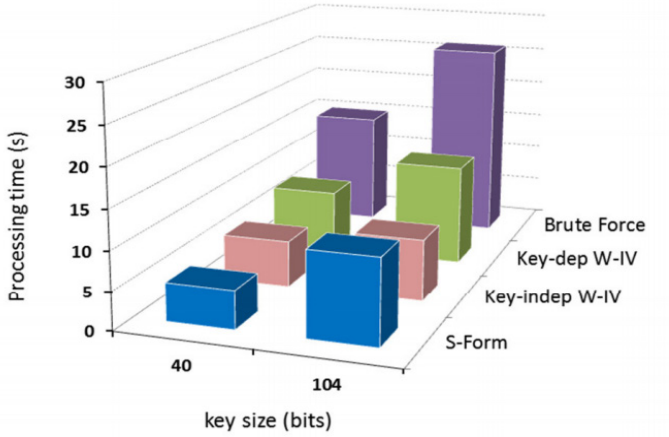


Рисунок 4. Изменение времени процессора с формой выбора

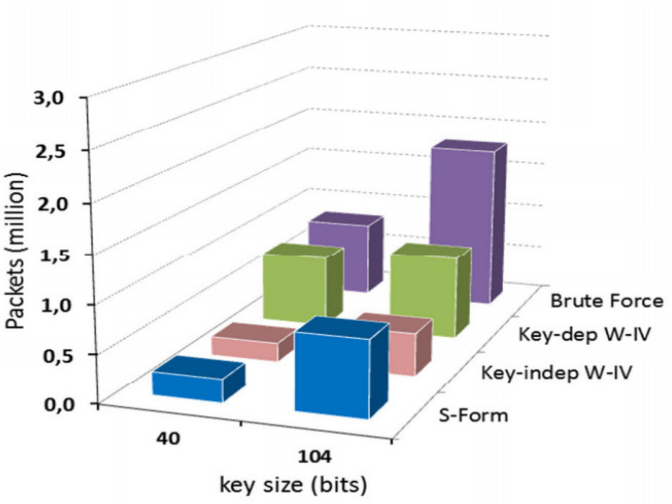


Рисунок 5. Вариация трафика, используемая с IV формой выбора

Примечательно, что независимый от ключа слабые пакеты превосходит другие формы. Кроме того, грубой силе требуется гораздо больше времени, чтобы улучшить свою производительность, особенно для ключа длиной 104 бита. Кроме того, оказывается, что и в той же среде независимый от ключа слабый IV в большинстве случаев значительно лучше. В целом, атака FMS доказала свою эффективность для атаки WEP. В целом, наш вклад с менее чем 0,2 миллионами пакетов и по сравнению с результатами, представленными в Таблице 2, представляется улучшенным способом значительного уменьшения размера данных, необходимых для успеха атаки FMS. Однако текущие исследования в области беспроводного криптоанализа направлены на атаки WPA и WPA2, которые остаются неэффективными до сегодняшнего дня.

Table 2. Summary of most popular alternatives of FMS attack

FMS attack	Amount of packets (million)	Success prob.
Fluhrer et al. [10]	4-6	100
Stubblefield et al. [11]	1-2	
Hilton [27]	1	
Tews et al [15]	0.7	50

Рисунок 6. Размеры данных, необходимых для успеха атаки FMS

Вывод: Протоколы Wi-Fi заявляют о предоставлении решения безопасности, такого как проводные сети; они по-прежнему представляют интерес до сегодняшнего дня. Однако такие протоколы не являются полностью безопасными и могут стать целью атак восстановления ключей в реальном мире. В этой статье мы пролили некоторый свет на поведение протокольных атак и продемонстрировали, что на практике они кажутся сложнее, чем в теории, и вероятность их успеха часто просчитывается и зависит от среды тестирования, которая различается в зависи-

мости от каждого вклада. Результаты в литературе не могут быть воспроизведены из-за отсутствия деталей среды, таких как особенности пакетов и настройки реализации, которые, кажется, воспринимаются эвристически. Наши эксперименты показывают, что FMS не является полной атакой восстановления ключа, но может быть улучшена путем хорошего сбора пакетов; Таким образом, независимая от ключа стратегия слабого кажется лучшим способом выбора слабых ключей и позволяет выявлять секретные ключи менее чем за 10 секунд в среднем с полмиллиона пакетов. На основании предыдущих результатов можно сделать вывод, что ключевая безопасность протоколов на основе алгоритма RC4 просто предотвращает произвольные уязвимости, но не против злоумышленников; Векторы инициализации кажутся самым слабым звеном в процессе безопасности. Алгоритм AES, основанный на протоколах, является более устойчивым к атакам, но его развертывание в активных сетях кажется слишком дорогим из-за их схемы шифрования (CCMP), которая требует изменений в аппаратном оборудовании.

Список литературы

1. Akyildiz I. F, Su W, Sankarasubramaniam Y and Cayirci E. Wireless sensor networks: a survey. Computer Networks 2002; 38:393-422.
2. IEEE Std 802.11a. Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. LAN/MAN Standards Committee of the IEEE Computer Society. 1999.
3. Rivest R. The RC4 encryption algorithm. RSA Data Security. 1992.
4. IEEE Std 802.11.Information Technology-Telecommunication and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11-Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.1997.
5. Edney J, William A. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Boston: Addison-Wesley Longman Publishing Co. 2003.
6. Ferguson N. Michael: an improved MIC for 802.11 WEP. IEEE doc. 802.11-2/020r0. 2002.
7. Housley R, Whiting D, Ferguson N. Alternate Temporal Key Hash. IEEE doc. 802.11-02/282r2. 2002.
8. Moen V, Raddum H and Hole K J. Weaknesses in the Temporal Key Hash of WPA. Mobile Computing and Communications Review, 2001. 76-83.
9. Borisov N, Goldberg I and Wagner, D. Intercepting mobile communications: The insecurity of 802.11. Chez MOBICOM, Rome, Italy, 2001.
10. Fluhrer S, Mantin I, Shamir A. Weaknesses in the key scheduling algorithm of RC4. Chez Annual Workshop on Selected Areas in Cryptography, Toronto, CA, 2001.

АДДИТИВНЫЕ ТЕХНОЛОГИИ В СТРОИТЕЛЬНОЙ ПРОИЗВОДСТВЕННОЙ СФЕРЕ

Богодухова Екатерина Сергеевна
студентка 2 курса Факультет машиностроения
Московский Политехнический университет

Кашапова Регина Фильзатовна
студентка 2 курса Факультет машиностроения
Московский Политехнический университет

Конюхова Галина Павловна
кандидат педагогических наук, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»

Аннотация: *в данной статье описано исследование аддитивных технологий в промышленном производстве. Спроектирована модель - макета строительного робота. Приведены основные характеристики данного изобретения. А так же представлен проект по модернизации строительного 3D - принтера.*

Ключевые слова: *строительный 3D - принтер, аддитивные технологии, роботостроение.*

Abstract: *describes the research of additive technologies in industrial production. The model of the construction robot is designed. The main characteristics of this invention are provided. And the project on modernization construction 3D - the printer is also submitted.*

Keywords: *3D building printer, additive technologies, robot building.*

В современном производстве все большую популярность набирает такое молодое развивающиеся направление, как аддитивные технологии (АМ). АМ – это чрезвычайно востребованная технология послойного изготовления объекта на основе 3D – моделирования в различных производственных сферах. Применение ей нашлось и в строительной индустрии, где она заменяет традиционные методы строительства, позволяя значительно облегчить ряд производственных этапов [1]. Основная проблема данных высокоскоростных процессов, на сегодняшний день, - это ограниченность в применении, именно поэтому был разработан проект «Construction 2025», целью которого является углубленное применение АМ-технологий в строительстве. Достигнуть ее помогут несколько задач:

- Изучить аспекты АМ-технологий в строительстве.
- Проанализировать достижения нескольких стран по внедрению аддитивных технологии в производственную сферу.

Произвести расчётный анализ и представить проект «Construction 2025».

Строительство является одной из самых ресурсозатратных отраслей производства. По экономическим показателям оно расходует около 42% сырьевых материалов и, тем не менее, имеет малую производительность. Таким образом, применение 3D-технологий позволит снизить техногенную нагрузку на окружающую среду и сэкономить до 90 % исходного материала в отличие от текущего традиционного производства. Так же АМ подразумевает под собой автоматизированные системы, позволяющие создавать строительные объекты сложной геометрической формы, с целью замены ручного труда [2].

Такая страна, как Северная Америка, по данным

за 2018 год, остается крупнейшим потребителем аддитивных технологий в мире (Рис. 1). В Техасе

представили комфортабельный дом, напечатанный на 3D принтере. Уникальная особенность этого объекта, площадью 68 заключалась в том, что на сам процесс создания постройки ушло 48 часов, а стоимость составила 4 тысячи долларов. Номер в гостиничном комплексе в Филиппинах высотой 4 метра и площадью – 120 был построен за 100 часов. На его территории есть 2 номера и ванна-джакузи. «Офис будущего» в Дубае – одноэтажное здание площадью 250 , этот проект был выполнен за 17 дней (Табл. 1) [3].

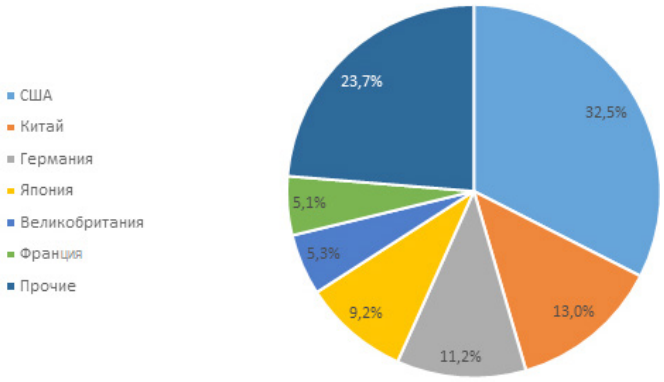


Рисунок 1 - Диаграмма потребителей АМ-технологий в мире

На основании произведенного анализа были выявлены следующие преимущества аддитивных технологий в строительстве:

Экономия. Уменьшение срока строительства, расхода материалов.

Экологичность. Минимизируется количество вредных отходов от строительства.

Качество. Точные данные, заложенные программой, исключение человеческого фактора.

Таблица 1 – Параметры строительных 3D - моделей

Страна	Площадь, S	Время, t, Ч	Стоимость, P, $
Техас	68	48	4 000
Филиппины	120	100	60 000
Дубай	250	408	140 000
Китай	4305	1080	110 850

Проект «Construction 2025» представляет разработку усовершенствованной модели строительного робота с функцией 3D - печати. Робот состоит из корпуса на самоходном шасси, встроенного в него бортового компьютера и 3D - принтера, где два экструдера расположены в нижних частях стрел перпендикулярно строительным манипуляторам. Универсальность данного изобретения заключается в том, что оно работает с кирпичными блоками, внешне напоминающими детский конструктор «Лего», соединяя их между собой с помощью специальной смеси.

Работа «Construction 2025» осуществляется таким образом: в 3D-принтер загружается 3-х мерная компьютерная модель будущего строительного объекта, бортовой компьютер относительно нее определяет расположение каждого блока, его привязку по высоте, по глубине и последовательности укладки. Исполнителями данной программы являются экструдеры, которые наносят готовую строительную смесь на основание, а впоследствии и на каждый кирпичный блок, поставленный манипуляторами. Такой раствор включает в себя следующие компоненты: стекло, сталь, цемент и фиброволокно, которое не позволяет появляться трещинам и значительно увеличивает прочность. Следует отметить, что в отличие от традиционного метода проект «Construction 2025» имеет колоссальные преимущества (Табл.2) [4].

Таблица 2 – Преимущества проекта «Construction 2025»

Стоимость в % от традиционного строительства	Основной вклад	С применением проекта «Construction 2025»
На 20-30% дешевле	Финансирование	Короткая продолжительность проекта с быстрым выходом на рынок резко снижает стоимость проекта
На 25-35% дешевле	Материалы	Отсутствие строительных отходов
На 45-60% дешевле	Работа	Существенное снижение ручного труда, так как физическая работа заменяется цифровыми технологиями

Таким образом, были изучены попытки по внедрению роботизации в строительство, направленные на автоматизацию. Основываясь на данных исследованиях, была спроектирована модель «Construction 2025», сравнительный расчетный анализ показал экономическую прибыльность с ее использованием.

На данный момент рынок трехмерной печати далек от перенасыщения. Именно поэтому аддитивные технологии имеют огромные перспективы в производственно-потребительской сфере без наличия конкурентоспособных компаний.

Список литературы:

1. Э. Канесса, К. Фонда, М. Зеннаро Доступная 3D печать для науки, образования и устойчивого развития. – М.: Издательство ICTP, Италия, 2013 - с.61.
2. Аддитивные технологии в строительстве [Электронный ресурс] // Сайт о строительстве и производстве. URL: http://www.3dpulse.ru/ (дата

обращения: 22.03.2019)
3. Аддитивное производство [Электронный ресурс] // Сайт о перспективах аддитивных технологий. URL: http://www.tadviser.ru/ (дата обращения: 22.03.2019)
4. Строительные 3D-принтеры [Электронный ресурс] // Сайт об опыте работы со строительными принтерами. URL: http://3dtoday.ru (дата обращения: 24.03.2019)

ИЗМЕНЕНИЯ ТРУДОВЫХ РЕСУРСОВ В ГОРОДАХ С АЭС НА ПРИМЕРЕ Г. ОСТРОВЕЦ, РФ

Рубцов Артем Михайлович
студент 2 курса, направления «Информатика и вычислительная техника», Московского политехнического университета,

Чабаненко Екатерина Борисовна
старший преподаватель кафедры «Инфокогнитивные технологии» Московского политехнического университета

Аннотация: *В статье проанализированы изменения в г. Островец от периода начала строительства АЭС до 2019 года. Официальная миграционная статистика. Количество и качество кадров, переезжающих в Островец.*

Ключевые слова: *Россия, Белоруссия, АЭС, Островец, Гродненская область, изменения в Островце.*

Abstract: *The article analyzes the changes in the city of Ostrovets from the start of construction of nuclear power plants until 2019. Official migration statistics. The number and qality of personnel moving to Ostrovets.*

Keywords: *Russia, Belarus, NPP, Ostrovets, Grodno region, changes in Os-trovets.*

Первое упоминание об Островце датируется 1468 г., и вплоть до 2012 года Островец являлся городским поселком, не имея статуса города. Как и большинство постсоветских городов, с 90-ых годов население города уменьшалось [1]. Изменился статус городского поселка на город из-за начала строительства Белорусской АЭС в конце 2011 года, рядом с Островцом. По данным Белстата (Таблица 1) [2], население сократилось с 31100 человек в 1996 году до 24024 человек в 2011. Тенденция на снижение численности населения сохраняется почти по всем районам Гродненской области, за исключением г. Гродно и Островецкого района.

Однако население г. Гродно увеличивается за счет миграции из Гродненской области, т.к. в этом городе высокий уровень жизни по стране (Республика Беларусь), мигрирует в основном молодежь.

В Островецком районе ситуация обстоит иначе. В этот населенный пункт переезжают преимущественно люди, вовлеченные в строительство Белорусской АЭС, преимущественно граждане, проживающие в крупных городах Беларуси, а также граждане России. В постройке Белорусской АЭС заняты 41 подрядная организация (23 - белорусские, 18 - российские). Численность строительного персонала составляет около 7 тыс. человек [3].

За счет технологической сложности построения АЭС, приезжают люди, имеющие образование. Так как зарплатные ожидания и требования к уровню жизни у сотрудников АЭС выше, чем у местного населения, город стремительно развивается. Прогнозируется рост населения в г. Островец с 10,3 тыс. человек до 25 тыс. человек [4].

Ввиду большого количества новоприбывших сотрудников АЭС, имеющих высокую покупательную способность увеличивается число новых рабочих мест для местного населения. Ведутся существенные, в масштабах этого города, работы по строительству жилья для сотрудников АЭС. Строительство ведется с привлечением сил местного населения. Для сотрудников, приезжающих в Островец на

Таблица 1. Население Гродненской области

	1 996	2 001	2 002	2 003	2 004	2 005	2 006	2 007	2 008	2 009
Гродненская область	1 204 100	1 170 125	1 160 218	1 147 982	1 135 387	1 122 058	1 107 903	1 096 170	1 086 048	1 076 799
г. Гродно	298 200	303 917	305 262	306 224	307 063	307 716	308 221	310 353	313 215	321 740
районы:										
Лидский	148 600	146 270	145 120	143 963	142 475	140 949	139 273	137 828	136 543	135 839
Ошмянский	38 500	36 676	36 321	35 749	35 257	34 630	33 993	33 409	32 951	32 592
Сморгонский	63 000	60 954	60 271	59 449	58 779	57 947	57 147	56 435	55 829	55 604
Гродненский	68 500	67 038	66 636	66 036	65 513	64 921	64 259	63 449	62 909	55 525

Продолжение таблицы

	2 010	2 011	2 012	2 013	2 014	2 015	2 016	2 017	2 018
Гродненская область	1 071 305	1 066 010	1 061 248	1 058 415	1 054 861	1 052 588	1 050 125	1 047 494	1 043 681
г. Гродно	330 311	338 287	346 601	352 485	356 557	361 352	365 610	368 710	370 919
районы:									
Лидский	134 907	133 972	133 295	133 027	132 678	132 291	132 114	132 099	131 860
Островецкий	24 187	24 024	24 111	23 936	23 929	23 826	23 792	24 243	24 554
Ошмянский	32 311	32 123	31 872	31 653	31 354	31 190	30 969	30 943	30 796
Сморгонский	55 064	54 658	54 081	53 775	53 533	53 113	52 608	52 166	51 930
Гродненский	54 104	52 708	51 254	50 542	50 002	49 830	49 954	49 987	49 803

короткий срок был построен комфортабельный отель с привлечением денег иностранных инвесторов. Среди сотрудников АЭС, постоянно проживающих в Островце, есть семьи с детьми. Для них были построены школы, а также детский сад. Открываются супермаркеты, магазины бытовой техники, кафе, рестораны, появляются банки. Стимулируется развитие малого и среднего бизнесы ввиду возросшего спроса. Тем самым местное население получает рабочие места. Улучшается инфраструктура между Островцом и крупными городами. На регулярной основе работают несколько перевозчиков, связывающие Островец с крупными городами Беларуси, Гродно и Минском.

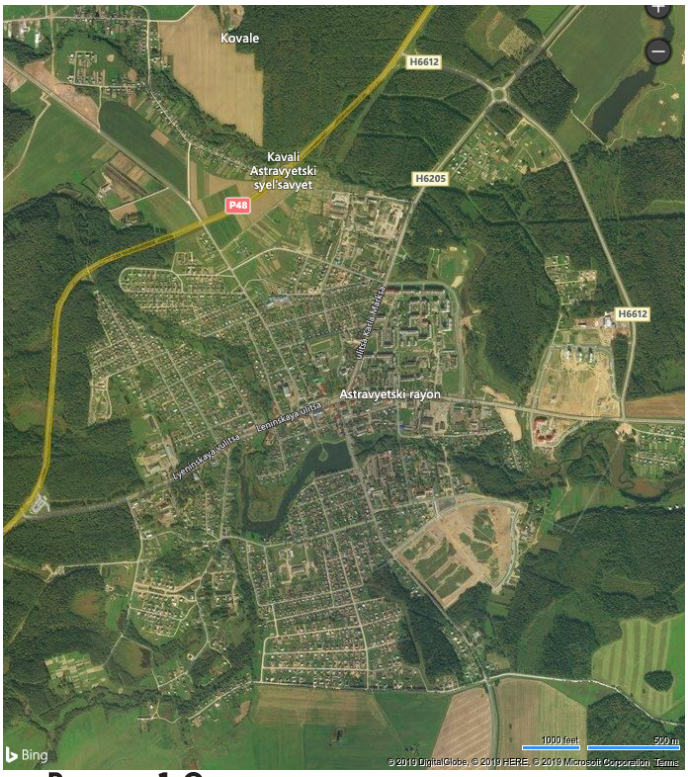


Рисунок 1. Островец до начала строительства БелАЭС. 2010 год. [5]

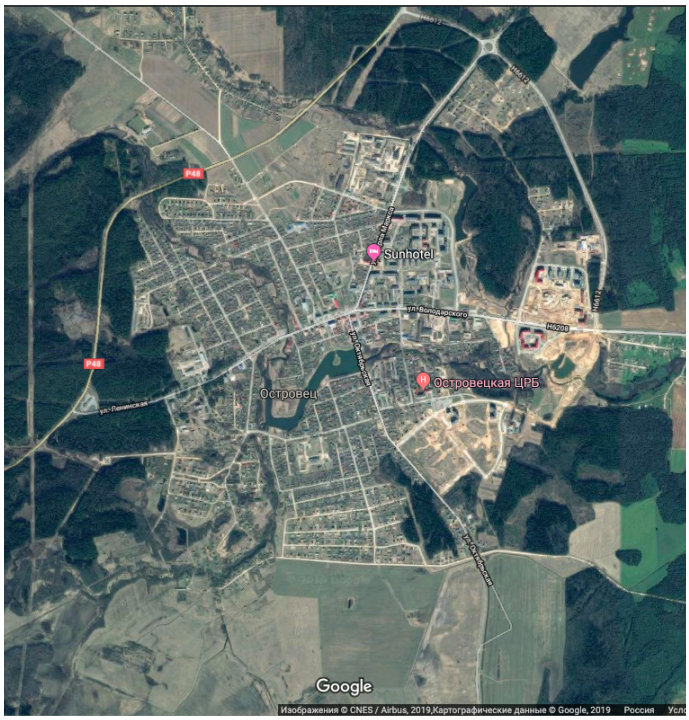


Рисунок 2. Островец на момент 2015 года. [6]

Однако у города появляется проблема характерная для всех городов с АЭС, миграция жителей, не вовлеченных в атомную энергетику. Это касается местного населения, преимущественно молодого, ввиду узкого рынка труда. Отток направлен на крупные города Беларуси и ближнего зарубежья.

Вывод: Появление АЭС благоприятно сказывается на экономическом развитии города, ввиду увеличения квалифицированного рабочего труда, который в свою очередь формирует вокруг

Рисунок 3. Островец в 2018 году. [7]

себя благоприятную среду для развития бизнеса, направленного на обеспечение должного уровня жизни людей, работающих в атомной энергетике. Однако будет сохраняться миграционный отток среди местного населения, особенно среди молодежи.

Список литературы

1. Лазаренко В. А. Социальное развитие городов атомной электроэнергетики России (на примере Десногорска) // Вестник Кемеровского государственного университета. 2018. No 1. С. 6-13. DOIl0.21603/2500-3372-2018-1-6-13.
2. Белстат: http://grodno.belstat.gov.by/
3. Белта: https://atom.belta.by
4. Издательский дом Беларусь Сегодня: https://www.sb.by/
5. Yahoo Maps. https://maps.yahoo.com/
6. Google Maps. https://www.google.ru/maps/
7. Яндекс.Карты. https://yandex.ru/maps

МЕТОДЫ ЗАЩИТЫ ДАННЫХ В WEB

Бабиков Алексей Константинович
Студент 4 курса, направление: Информационная безопасность Автоматизи-рованных систем, Московский Политехнический университет

Лушина Ольга Владимировна
Ассистент кафедры «SMART-технологий» Московского политехнического университета

Аннотация: *В статье описано применение протоколов SSL и TLS для защиты данных, передаваемых по средствам компьютерных технологий. Протокол SSL призван обеспечить возможность надежной защиты сквозной передачи данных с использованием протокола TCP. SSL представляет собой не один протокол, а два уровня протоколов. Протокол записи SSL (SSL Record Protocol) обеспечивает базовый набор средств защиты, применяемых протоколами более высоких уровней. Эти средства, в частности, может ис-пользовать протокол передачи гипертекстовых файлов (HTTP), призванный обеспечить обмен данными при взаимодействии клиентов и серверов Web*

Ключевые слова: *SSL, TLS, компьютерные технологии, протоколы*

Abstract: *the article describes the use of SSL and TLS protocols to protect data transmitted by means of computer technologies. The SSL Protocol is de-signed to provide reliable protection of end-to-end data transmission using the TCP Protocol. SSL is not a single Protocol, but two layers of protocols. SSL Record Protocol (SSL Record Protocol) provides a basic set of security features used by higher-level protocols. These tools, in particular, can use the hypertext transfer Protocol (HTTP), designed to provide data exchange when interacting with clients and web servers*

Keywords: *SSL, TLS, computer technologies, protocols*

Введение. В связи с развитием информационных технологий необходимо улучшать меры защиты информации от различных атак.

Цель исследования: изучить криптографические протоколы

Задачи исследования:

- Рассмотреть принципы работы протоколов
- Проанализировать историю развития техно-логии

SSL («Secure Socket Layer») – криптографический протокол, который использует ассиметричную криптографию, симметричное шифрование и коды аутентификации для защиты передаваемых данных [2].

TLS («Transport Layer Security») – усовершенствованная версия протокола SSL, основанная на TLS версии 3.0 [1].

Оба эти протокола делают невозможным осуществление несанкционированного доступа и прослушивание пакетов, передаваемых по сети. На рисунке 1 представлено отличие защищённого соединение с сервером от незащищённого.

Рисунок 1. Защищённое соединение

Протоколы SSL и TLS применяют в тех случаях, где необходимо обеспечить надлежащий уровень защиты данных, передаваемых пользователем по сети. Например, для сайтов, которые используют платёжные системы или электронные кошельки, эти алгоритмы используются для защиты от перехвата данных злоумышленниками.

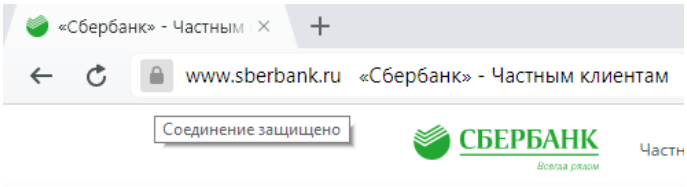


Рисунок 2. Защищённое соединение в платёжных системах

На рисунке 2 можно наблюдать наличие защищённого соединения на официальном сайте одного из наиболее популярных банков России.

История развития протоколов начинается с SSL версии 1.0, разработанным компанией «Netscape Communications» . Далее развитие история развития технологии защиты представлена на рисунке 3.

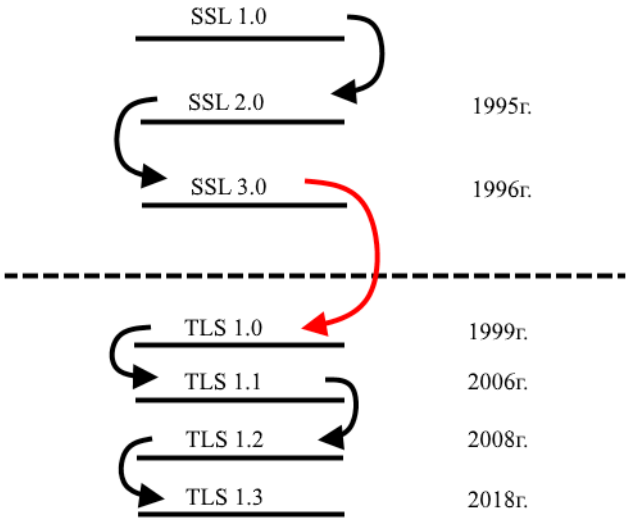


Рисунок 3. История развития технологии

Принцип работы данных протоколов заключается в том, что они выступают в роли фильтров для защиты данных при переходе с прикладного уровня на транспортный уровень в модели «TCP/IP», что изображено на рисунке 4.

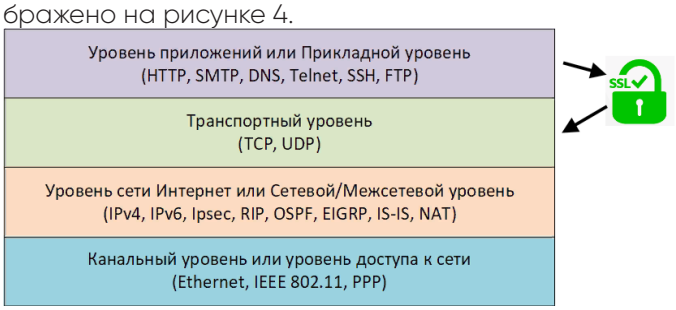


Рисунок 4. Защита данных в модели TCP/IP

Для шифрования данных используются ключи разной длины. Надёжность защиты напрямую зависит от этого ключа. Для наиболее важной информации используются ключи, длиной 128 бит. С их помощью возможно обеспечить надлежащий уровень защиты данных [1].

Для передачи на сервере необходимо присутствие SSL-сертификата, содержащего сведения о владельце ключа, о центре сертификации, данные об открытом ключе.

При наличии сертификата на сервере передача данных будет происходить следующим образом:

1. Обмен сообщениями инициализации
2. Обмен сертификатами и ключевым сообщением
3. Обмен секретными данными

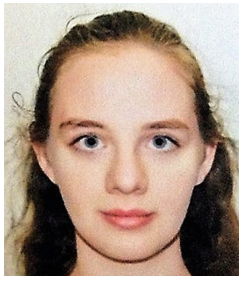
Основной особенностью использования SSL и TLS протоколов называется «прозрачность использования». Под этим понятием подразумевается возможность использовать эту защиту данных поверх любых приложений прикладного уровня [2].

Вывод. Изучив протоколы SSL и TLS можно удостовериться в необходимости применения такой технологии для обеспечения надлежащей защиты данных при передаче конфиденциальной или иной секретной информации. Процессы защиты информации, шифрования и дешифрования связаны с кодируемыми объектами и процессами, их свойствами, особенностями перемещения. Такими объектами и процессами могут быть материальные объекты, ресурсы, товары, сообщения, блоки информации, транзакции (минимальные взаимодействия с базой данных по сети). Кодирование кроме целей защиты, повышая скорость доступа к данным, позволяет быстро определять и выходить на любой вид товара и продукции, страну-производителя и т.д. В единую логическую цепочку связываются операции, относящиеся к одной сделке, но географически разбросанные по сети.

Список литературы

1. Титоренко Г.А. Информационные технологии управления. М., Юнити: 2002.
2. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика, Электронинформ, 1997

ВЛИЯНИЕ КУРОРТНОГО СБОРА НА РАЗВИТИЕ ТУРИЗМА В РОССИИ



Шарифуллина Алина Игоревна
студентка бакалавриата Финансового университета при Правительстве Рос-сийской Федерации

Молчанова Наталья Петровна
д.э.н., доцент, профессор Департамента общественных финансов Финансового университета при Правительстве Российской Федерации

Аннотация: *Исследуются причины разногласий среди экспертов ту-ристской индустрии по поводу принятого в 2017 году решения о введении курортного сбора в некоторых регионах России. Проведен анализ послед-ствий данного решения и вероятного возникновения рисков, которые могут препятствовать развитию туризма в России. Сформулированы рекомендации по преодолению возможных неблагоприятных для сферы туризма послед-ствий.*

Ключевые слова: *туризм, налог, курортный сбор, благоустройство, курортная инфраструктура.*

Abstract: *The reasons of disagreements among experts of the tourist indus-try concerning the decision made in 2017 on introduction of resort collecting in some regions of Russia are investigated. The analysis of the consequences of this decision and the likely occurrence of risks that may hinder the development of tourism in Russia. Recommendations for overcoming possible adverse conse-quences for the tourism sector are formulated.*

Keywords: *tourism, tax, resort fee, landscaping, resort infrastructure.*

Актуальность темы исследования. В научной литературе выделяются различные виды туризма по сфере распространения: внутренний, выездной, въездной. Проблемы регулирования развития внутреннего туризма обладают высокой актуальностью и исследуются учеными разных специальностей. Наибольший интерес представляют экономические и финансовые аспекты организации и планирования туристской деятельности [2]. По цели поездки различаются следующие виды туризма: рекреационный (медицинский), экскурсионный, научный, деловой, этнический, спортивный, религиозный, лингвистический и др. Основываясь на разнообразии природно-климатических условий нашей страны и результатах российских исследований, можно сделать вывод о закономерном росте интереса и популярности медицинского туризма [3]. Введение и регламентация курортного сбора вызывают разногласия не только среди потребителей туристских услуг, но и во всей туристской индустрии, что связано с его негативным восприятием как налога и путешественниками, и представителями туристического бизнеса. Цель данной работы – изучить влияние курортного сбора на российский рынок туристских услуг с помощью анализа законодательной базы, статистической информации и вторичной информации в СМИ.

Результаты выполненного анализа. Курортный сбор – это обязательная плата, взимаемая с туристов, приезжающих на определенный туристский объект, с целью поддержания действующей инфраструктуры: например, модернизация курортных зон, финансирование природоохранных мероприятий, улучшение сервиса, реконструкция памятников истории и архитектуры.

Практика курортного сбора распространена во всем мире. Например, в городе Санта-Моника (США) курортный сбор составляет 14% от общей суммы, уплаченной за аренду номера в средстве размещения. Этот налог является дополнительным источником дохода для города. В 2017 году туризм принес $1,96 млрд в местную экономику Санта-Моники, из которых более чем $54 млн поступило непосредственно от курортного сбора [9]. Также обязательна оплата курортного сбора во многих других странах, например, в Греции, Испании, Франции, Италии, Германии.

В Советском Союзе практика применения курортного сбора существовала с 1933 г. В

современной России закон о курортном сборе действовал с 1991 по 2004 год, но затем был отменен в связи с принятием решения об облегчении налогового бремени населения [1]. В 2017 году был подписан Федеральный закон от 29.07.2017 № 214-ФЗ «О проведении эксперимента по развитию курортной инфраструктуры в Республике Крым, Алтайском крае, Краснодарском крае и Ставропольском крае». Согласно данному нормативному правовому акту, курортный сбор взимается в четырех регионах России: с 1 мая 2018 года – с туристов, останавливающихся в коллективных средствах размещения в некоторых курортных городах Алтайского и Ставропольского краев; с 16 июля – в Краснодарском крае [4]. Изначально планировалось ввести налог с 1 мая 2019 г. в республике Крым, но в апреле 2019 года глава республики заявил об отказе введения курортного сбора в регионе. Если опыт курортного сбора будет положительным, через пять лет его предполагается ввести по всей стране.

В 2018 году размер курортного сбора не мог быть больше 50 рублей в сутки. Краснодарский край установил курортный сбор в размере 10, Ставропольский край – 50, Алтайский край – 30 рублей в сутки. Предусматривается, что в последующие годы размер курортного сбора не будет превышать 100 рублей с одного человека в сутки [5]. Сейчас Краснодарский край – это единственный регион, где предусмотрен штраф за уклонение от уплаты взноса: для граждан в размере от 500 до 2000 рублей, для операторов до 15000 рублей. Плательщиками курортного сбора являются физические лица, достигшие 18 лет, проживающие в объектах размещения более 24 часов, за исключением граждан, освобождённых от уплаты в соответствии с законодательством [1].

По официальным данным, всего с мая по октябрь 2018 года было собрано около 260 млн рублей в трех регионах России, которые приняли участие в эксперименте по взиманию туристского сбора. Из них более 140 млн рублей собрано в Ставропольском крае, около 98 млн – в Краснодарском крае, более 15 млн – в Алтайском крае. Общее количество туристов, заплативших налог, достигло 1,5 млн человек [6]. Все средства, полученные от уплаты курортного сбора, перечисляются в Фонд развития курортной инфраструктуры.

Средства из Фонда направляются исключительно на финансовое обеспечение работ по проектированию, строительству, реконструкции, содержанию и благоустройству объектов курортной инфраструктуры региона. По данным министерства РФ по делам Северного Кавказа, в 2018 году по итогам третьего квартала 54 миллиона рублей было направлено на благоустройство парка «Курортный» в Ессентуках, около 28 миллионов - на ремонт терренкура санатория «Горный воздух» в Железноводске, 37 миллионов рублей выделено на благоустройство парка «Цветник» в Пятигорске [7]. При этом курортный сбор не отменяет государственную поддержку регионов, а лишь дополняет ее. Однако, финансовое покрытие расходов, возникающих в связи с проведением эксперимента, осуществляется за счет средств бюджета данного субъекта.

Согласно статистическим данным, отношение российских туристов к курортному сбору отрицательное. Об этом свидетельствует опрос, проведенный сервисом по продаже железнодорожных и авиабилетов Biletix среди своих пользователей о том, повлияет ли введение курортного сбора на отечественных курортах в размере, не превышающем 100 рублей в сутки, на их выбор дестинации. По результатам исследования было установлено, что только 2,5% респондентов выразили согласие с введением курортного сбора и готовы его заплатить (рис. 1) [8].

В связи с неготовностью туристов платить данный сбор, существует ряд угроз, которые могут возникнуть при введении курортного сбора. Во-первых, может произойти увеличение процента отдыхающих в частном секторе, где налог не взимается. Во-вторых, многие представители туристского бизнеса высказываются против нововведения. Среди

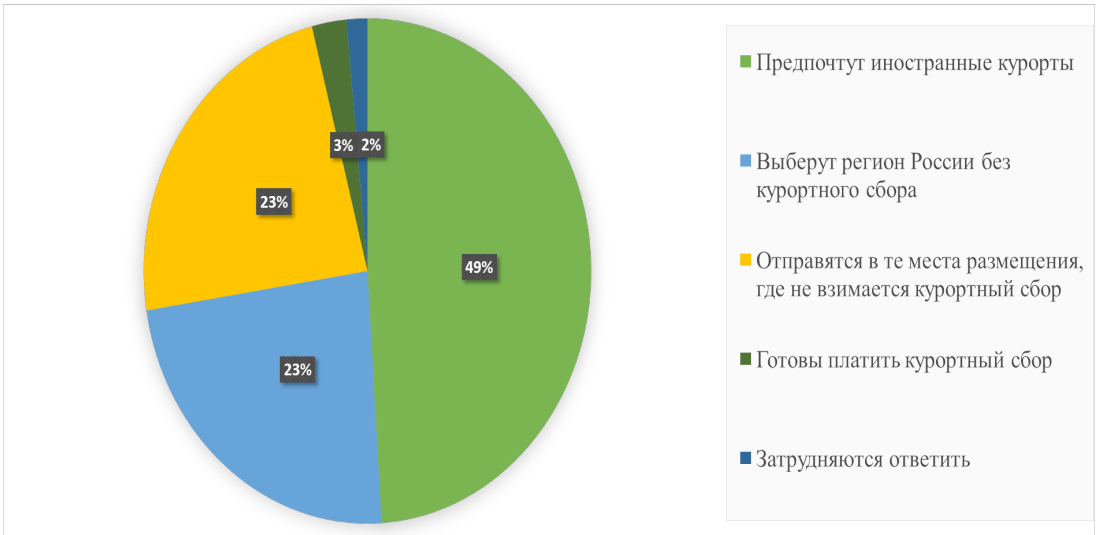


Рисунок 1 – Результаты опроса о введении курортного сбора

аргументов, которые они приводят, – неизбежный рост цен на путевки, что может оттолкнуть потенциальных туристов. В-третьих, эксперты обеспокоены тем, что схема сбора и использования средств детально не прописана. По предварительным оценкам, доходы от курортного сбора могут пополнить бюджеты регионов до 500 млн руб. в год, при этом для семьи из четырех человек (двух взрослых и двух детей) расходы на отдых в количестве 10 дней в регионе с курортным сбором 50 руб. в сутки увеличатся на 1000 руб. Как представляется, в контексте общих значительных расходов на путешествие в целом эта сумма не должна стать главным препятствием для принятия решения о выборе дестинации. Вместе с тем эти средства могут стать эффективным инструментом улучшения инфраструктуры туристических зон.

Заключение. Несмотря на все возможные угрозы, курортный сбор может стать одним из способов получения муниципальными образованиями финансовых средств для развития туризма, при выполнении следующих рекомендаций:

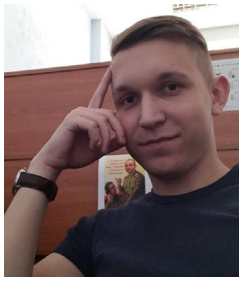
- проведение комплексного обследования имеющихся в регионе коллективных средств размещений с целью получения актуальных данных для оценки их текущего состояния и формирования соответствующей информационной системы;
- проверка состояния туристской инфраструктуры для выявления приоритетных направлений расходования средств;
- подробного ознакомления туристов с курортным сбором, порядком и целями его взимания на стадии принятия решения о предстоящем путешествии. Однако на начальных этапах стоит включать налог в цену гостиничного номера.
- организация постоянного мониторинга сбора и расходования денежных средств, взимаемых с туристов.

Таким образом, введение туристского сбора, его правильное администрирование и расходование полученных средств по целевому назначению, по нашему мнению, будет способствовать повышению качества отдыха приезжающих и, впоследствии, может стать одним из факторов, способствующих повышению количества отдыхающих в туристских дестинациях.

Список литературы

1. Демьяненко Е. А. Курортный сбор с туристов РФ как способ обеспечения отрасли. Возможные проблемы и перспективы // Юридические науки: проблемы и перспективы: материалы VI Международной научной конференции. – Казань: Бук, 2017. С. 21-23.
2. Молчанов И.Н., Молчанова Н.П. Финансирование формирования и развития региональных туристских кластеров /В сб.: Социально-экономические проблемы развития отдельных отраслей сферы услуг. Москва, 2017. С. 109-118.
3. Молчанов И.Н. Медицинский туризм: роль в поддержании здоровья и увеличении продолжительности жизни населения //Экономика. Налоги. Право. 2019. №2. С. 127-136.
4. Федеральный закон №214-ФЗ от 29.07.2017 «О проведении эксперимента по развитию курортной инфраструктуры в Республике Крым, Алтайском крае, Краснодарском крае и Ставропольском крае».
5. Dzhandzhugazova E. A. Resort fee introduction in Russia in the focus of public debate // Espacios. 2018. T. 39. № 22. P. 8.
6. Сайт Интерфакс (дата публикации 22.11.2018) – [Электронный ресурс]. – Код доступа: https://tourism.interfax.ru/ru/news/articles/54271 (дата обращения 23.03.19).
7. Сайт Министерства РФ по делам Северного Кавказа – [Электронный ресурс]. – Код доступа: http://www.minkavkaz.gov.ru/kurortnyy-sbor/ (дата обращения 18.03.19).
8. Сайт РИА Новости (дата публикации 10.08.2017) – [Электронный ресурс]. – Код доступа: https://ria.ru/tourism/20170810/1500135762.html (дата обращения 19.03.19).
9. Сайт туризма и путешествий города Санта-Моника (дата публикации 25.05.2018) – [Электронный ресурс]. – Код доступа: https://www.santamonica.com/tourism-dollars-infuse-1-96-billion-santa-monicas-economy-2017/ (дата обращения 20.03.19).

ЗАЩИТА ИНФОРМАЦИИ В ВЫДЕЛЕННЫХ ПОМЕЩЕНИЯХ НА ПРЕДПРИЯТИИ



Ланин Сергей Павлович
Студент 4 курса, направление: Информационная безопасность Автоматизированных систем, Московский Политехнический университет

Ковалёва Анастасия Александровна
старший преподаватель кафедры «Инфокогнитивные технологии», Московского политехнического университета

Аннотация: *в статье описаны технические каналы утечки информации и некоторые методы по избеганию утечки этой информации.*

Ключевые слова: *выделенные помещения, ОТСС, ВТСС, СЗИ, НСД.*

Abstract: *the article describes the technical channels of information leakage and some methods to avoid the leakage of this information.*

Keywords: *allocated premises, OTSS, VTSS, SPI, NSD.*

Введение: В наши дни в серьезных организациях особенно остро стоит проблема защищенности информации от посторонних лиц, в следствии чего появляется все больше компаний и специалистов, компетентных в этих вопросах.

Речь будет идти исключительно о выделенных помещениях. Под выделенным помещением (далее – ВП) понимается помещение, предназначенное для проведений переговоров, собраний и других мероприятий, на которых обсуждается секретная или конфиденциальная информация. В первую очередь, к таким помещениям относятся переговорные комнаты в организациях, в которых происходят мероприятия речевого характера по конфиденциальным вопросам.

Следует отметить, что на данный момент ВП является хорошим показателем серьезности организации, к вопросам защищенности информации. В следствии чего будет интересно и полезно рассмотреть вопросы защиты информации в таких ВП, прежде всего говоря о переговорных комнатах.

Цель исследования: изучить концепцию построения СЗИ в выделенных помещениях.

Задачи исследования:

1) Рассмотреть технические каналы утечки информации;

2) Проанализировать способы несанкционированного доступа к информации закрытого характера;

3) Разработать рекомендации по обеспечению защищенности ВП.

На рисунке 1 представлена схема главных задач в обеспечении безопасности информации является защита информации от:

Рисунок 1. Задачи обеспечения БИ

1. От утечки по акустическому каналу (АК).
2. От утечки по виброакустическому каналу (ВАК).
3. От утечки за счет электроакустического преобразования (ЭАП).
4. От утечки за счет ВЧ-навязывания (ВЧН).
5. От утечки по оптическому каналу (ОК) [1].

Построение модели угроз и нарушителей для конфиденциальной информации, которое имеет большое значение при проведении переговоров в выделенных помещениях и не только. Разрабатывать модели угроз и нарушителей целесообразно опираясь на поставленные задачи защиты.

На рисунке 2 описаны некоторые виды утечки в акустическом канале:

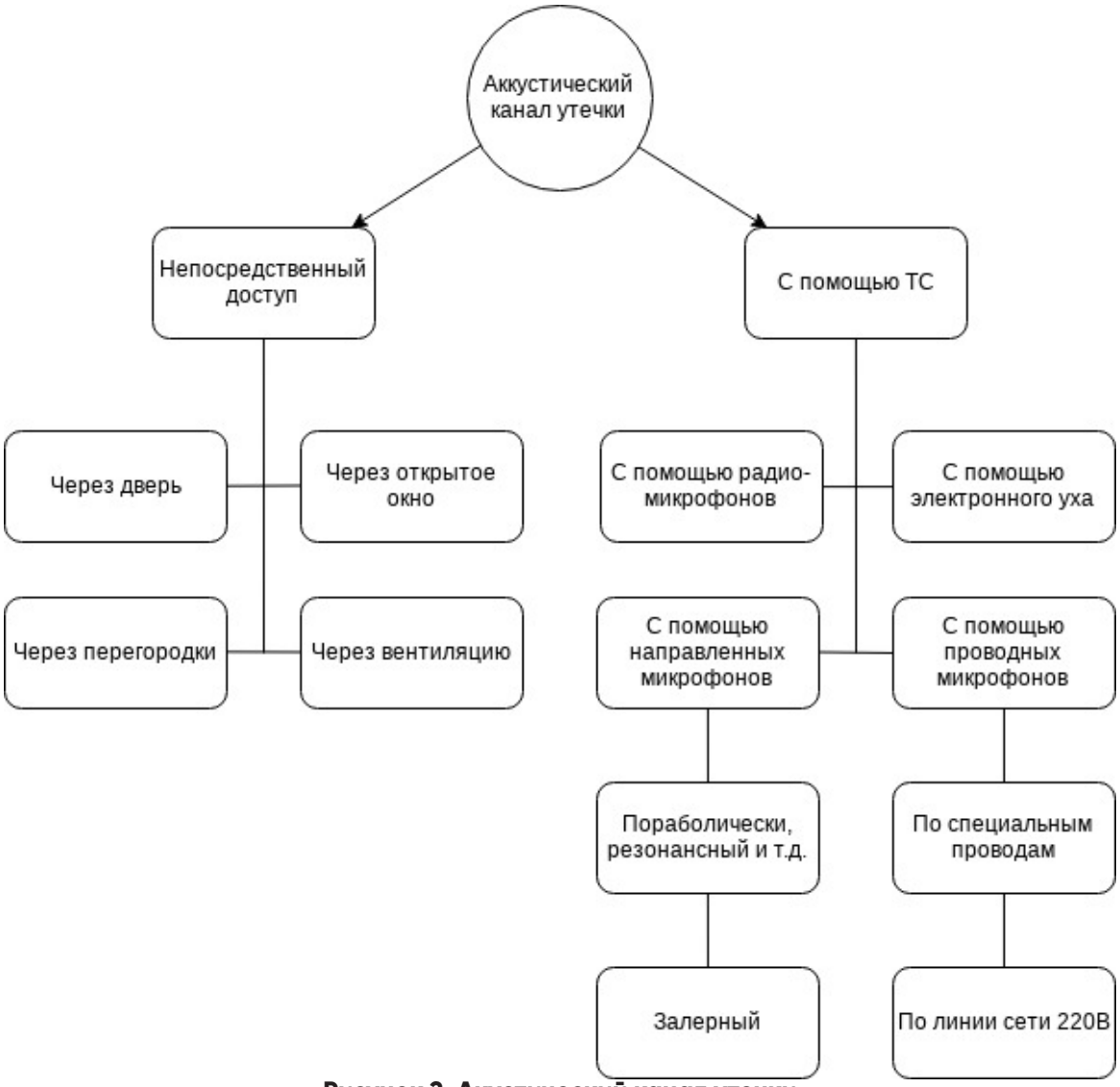


Рисунок 2. Акустический канал утечки

НСД к информации для служебного пользования может осуществляться путем:

- Непосредственного прослушивания;
- С помощью технических средств.

Переговоры можно «подслушать» если не закрыто окна или дверь, либо даже они закрыты, они могут не соответствовать звукоизоляционным нормам. Так же многие ошибочно считают, что потолок, стены и пол служат звукоизоляционными средствами, но ничто из перечисленного не является гарантированной защитой от утечки информации и тут стоит уточнить, если спецпроверки не проводились в принципе - никаких гарантий быть не может.

В настоящее же время злоумышленниками широко используются направленные микрофоны. При всем этом дистанция прослушивания вполне может достигать сотни метров.

В качестве направленных микрофонов злоумышленники часто используют:

- с параболическим отражателем
- резонансные
- щелевые
- лазерные

Более подробные технические характеристики перечисленных микрофонов достаточно полно представлены в интернете и необходимой литературе [2].

На рисунке 3 описано то, как несанкционированный доступ может быть осуществлен:

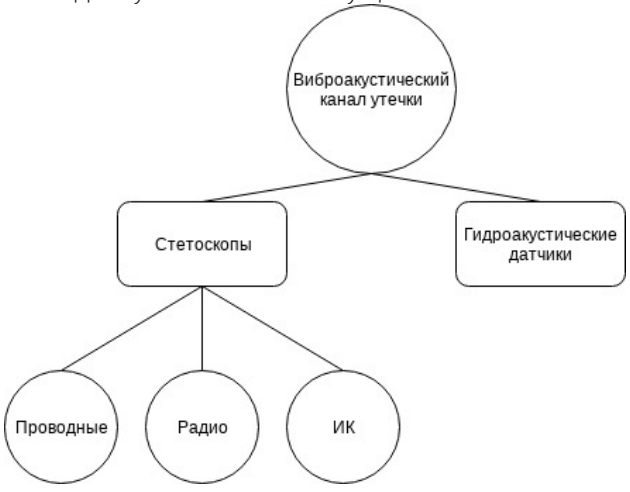


Рисунок 3. Виброакустический канал утечки

С помощью стетоскопов можно прослушивать стены толщиной до 20 сантиметров, в зависимости от

материала.

Утечка информации для служебного пользования возможно так же благодаря тому, что воздействие звуковых колебаний на элементы электрической схемы вспомогательных технических средств. В профессиональной среде такие технические средства (далее- ТС) принято обозначать как ВТСС.

К таким ТС относятся те, которые не принимают непосредственное участие в обработке информации, но могут быть причиной ее утечки.

На рисунке 4 представлены некоторые возможные каналы утечки за счет ВТСС:

Рисунок 4. Каналы утечки за счет ЭАП и ГО

Такие каналы возможно, если в комнате присутствуют телефонные аппараты, телевизор, электрические часы, приемники и так далее.

Рекомендации по защите:

Для начала необходимо сформулировать задачи и поставить цели. После этого необходимо выявить все каналы утечки информации, путем составления модели угроз и нарушителей.

Потенциальный нарушитель хорошо осведомленный человек, поэтому нужно сразу реализовывать комплекс средств защиты информации.

Очень важен контроль соответствия нормативным документам по ЗИ, и для этого необходима аттестационная комиссия, которая может указать на найденные недостатки и, по мере их полного устранения, - выдать аттестат соответствия.

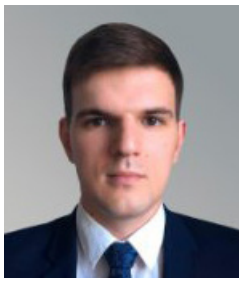
Список литературы

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005, с. 416.

2. Положение по аттестации объектов информатизации по требованиям безопасности информации. (Утверждено Председателем Гостехкомиссии России 25.11.1994). – М.: Гостехкомиссия РФ, 1994, с. 22.

МЕТОДЫ ПРОДВИЖЕНИЯ НА РЫНОК ВЫСОКОТЕХНОЛОГИЧНОЙ ПРОДУКЦИИ В СОВРЕМЕННЫХ УСЛОВИЯХ.

Устинова Лилия Николаевна
д.э.н., профессор каф. УИиКИС
Российская государственная академия интеллектуальной собственности



Роман Николай Павлович
аспирант 2 курса
Российская государственная академия интеллектуальной собственности

Аннотация: *В данной статье систематизированы и представлены стратегии продвижения на рынок высокотехнологичной продукции, с учётом современных рыночных условий, так же изложены методы и комбинации передачи, внедрения, продвижения технологий, форма которых зависит от особенностей высокотехнологичной продукции. Отражена роль цифровых технологий при принятии управленческого решения в выборе ценностного сегмента рынка. При написании были проанализированы труды как российских, так и зарубежных ученых-экономистов.*

Ключевые слова: *высокотехнологичный продукт, продвижение, цифровые технологии, методы и стратегии продвижения, инновации, внедрение, коммерциализация, инвестиции, НИОКР.*

Abstract: *This article systematizes and presents strategies for the promotion of high-tech products to the market, taking into account current market conditions, as well as outlines the methods and combinations of transfer, implementation and promotion of technologies, whichshapedepends on the characteristics of high-tech products. The role of digital technologies in managerial decision-making in the choice of the market value segment is reflected. When writing, the works of both Russian and foreign economists were analyzed.*

Keywords: *High-tech product, promotion, digital technologies, methods and strategies of promotion, innovation, implementation, commercialization, investment, R & d*

Введение.

Актуальность темы

Для повышения конкурентоспособности предприятий основное внимание уделяется созданию и распространению высокотехнологичных товаров в производственной сфере, трансформировании результатов интеллектуальной деятельности в инновационные продукты и услуги, реализуемые на рынке.

Целью исследования является анализ и сопоставление методов продвижения на рынке высокотехнологичных товаров. Задачи исследования включают выявление потенциала российской промышленности для производства высокотехнологичной конкурентоспособной продукции на основе системных инноваций; повышения технологического уровня производства и формирования условий для опережающего инновационного развития.

Необходим переход от роста на основе эксплуатации имеющихся факторов производства к развитию наукоемкого производства, основанного на комплексе инновационных технологий и интеллектуального капитала как главных факторов конкуренции. Такая продукция обладает уникальными характеристиками, включающими технически сложные товары, произведенные на базе новейшей технологии, имеющие короткий жизненный цикл и ориентированные на удовлетворение потребностей развивающихся предприятий, и одновременно создающие рыночный спрос. Создание и развитие наукоемких производств, возможности воспроизводства инноваций напрямую зависят от их успеха на рынке.

Объектом исследования являются наукоемкие предприятия российской экономики.

Предмет исследования – управление продвижением результатов интеллектуальной деятельностью наукоемких предприятий.

Успешное внедрение наукоемкой разработки

как главный результат эффективного инновационного процесса требует многоступенчатого принятия управленческих решений.

Эффективная инновационная деятельность возможна при создании системы управления инновациями, включающая подсистемы управления инфраструктурой, знаниями, подсистемы технологического аудита.

Раскрыты новые стратегии взаимодействия с потребителями, учитывая особенности эксплуатации продукции у потребителей и конкуренцию на рынке.

Содержание

При продвижении высокотехнологичного продукта на рынок необходимо оценить его отличительные свойства, позволяющие получить высокий результат по сравнению с известными аналогами.

Экспертный анализ позволят создавать механизмы отбора результатов интеллектуальной деятельности, оценки качества исследований и разработок, перспектив их коммерческой реализации, что кардинально повысит ее конкурентоспособность в условиях нарастающей глобальной конкуренции. Цифровые технологии позволяют оперативно изучить ситуации во внешней среде, из альтернативных решений выбрать наиболее качественное решение. В цифровой экономике активно создается информационная инфраструктура, информационно-телекоммуникационные технологии, формируется новая технологическая основа в экономической сфере. Основные функции современных информационных технологий управления предприятиями - поиск, сбор, обработка, хранение необходимых данных, выработка новой информации, решение оптимизационных задач. В результате такой обработки первичной информации получается информация нового качества, на основе которой и вырабатываются оптимальные управленческие решения. Инновационная активность промышленности определяет возможности роста эффективности промышленного производства и перспективы конкурентоспособности промышленности.

Крупный бизнес обладает конкурентными преимуществами в эффективности инновационного развития. Госкомпании, занимая лидирующие позиции в наукоемких, инфраструктурных и топливно-энергетических отраслях, обеспечивают научно-технологический прогресс и экономический рост национальных экономик. Крупные госкомпании формируют современный рынок, рынок интеллектуальной собственности, создавая новые технологии, виды товаров и услуг на основе реализации программ инновационного развития, имеющих значительную финансовую поддержку, прежде всего, со стороны государства. Следует отметить, что большинство компаний лидеров корпоративного сектора осуществляют широкомасштабное финансирование НИОКР самостоятельно за счет собственной прибыли. Основными результатами проводимых НИОКР являются нематериальные активы - ключевые ресурсы развития организаций, способные обеспечить конкурентные преимущества в условиях современного инновационного процесса. В этой связи, актуален анализ динамики состояния НМА как основы научно-исследовательской и инновационной деятельности российских компаний с государственным участием при зарождении новых технологий в переходный период организационного развития.

Усиление конкуренции влечет за собой снижение цен и сокращение жизненного цикла товаров, что способствует снижению прибыльности отрасли и оказывает отрицательное влияние на инновационные возможности предприятия. В результате на высокотехнологичном рынке компании встречаются с серьезными проблемами, множество научно-исследовательских проектов не доводится до коммерциализации.

Высокотехнологичная продукция — это продукция, для производства которой используются сложные технологические процессы. Признаком сложности является то, что в высокотехнологичных отраслях продукция или технологические процессы основываются на результатах не только прикладных, но и фундаментальных научных исследований [1].

Достигнутый уровень инновационного развития высокоразвитыми странами в прошлом базировался на интенсивном международном технологическом обмене, использующего различные формы распространения любых научно-технических знаний и производственного опыта. В условиях транснациональных отношений доминирует рыночная форма обмена. Важным фактором, влияющим на характер рынка научно-технической продукции, остается такая форма организации НИОКР, которая обеспечивает интеграцию науки, образования и производства. Включают: передачу технологий на основе актов международного сотрудничества; в совместные предприятия; на основе лицензионной деятельности; услуги типа инжиниринг; межотраслевой обмен; создание совместных научных центров для исследования сложных проблем.

В последнее время отечественными производителями, выпускающими высокотехнологичную продукцию, все больше внимания уделяется изучению поведения потребителей, разработке индивидуальных технических решений для удовлетворения самых взыскательных потребностей. Но потребителям все сложнее разбираться в нарастающем многообразии предлагаемых новых продуктов, а производителям продвигать их на рынок.

Появляется необходимость обновления производства для выпуска конкурентоспособной продукции, а также поиску новых каналов реализации высокотехнологической продукции. Корпоративные информационные системы управления предприятием, базы данных предоставляют информацию о новых технологиях, производственном опыте и об измене-

ниях внешней среды. Интегрированные решения для управления ресурсами промышленных предприятий (системы ERP), цепочками поставок (SCM) и взаимоотношениями с клиентами (CRM) позволят повысить эффективность работы любого предприятия, улучшить обслуживание клиентов, организовать эффективное взаимодействие с партнёрами, синхронизировать работу цепочки поставок с колебаниями спроса, выполняя заказы или другие обязательства точно в намеченные сроки.

Продвижение на рынок высокотехнологичной продукции — довольно сложный и многостадийный процесс, предполагающий практическое использование результатов НИОКР с целью выведения на рынок новой или усовершенствованной продукции, процессов или услуг для последующего получения коммерческой прибыли [2]. Успешное внедрение высокотехнологичных разработок, как главный результат эффективного инновационного процесса, требует многоступенчатого принятия управленческих решений.

Наиболее распространенный подход к рассмотрению инновационного процесса отводит решающую в нем роль интерактивному взаимодействию создателей технологии с окружающей их внешней средой. В таком случае, модель внедрения инновации можно рассматривать как последовательную цепочку событий, состоящую из нескольких функционально связанных стадий, на каждой из которых исполнители инновационного проекта взаимодействуют с внешним научным сообществом, бизнес-средой и рынком.

Ключевым фактором, влияющим на характер рынка научно-технической продукции, является такая форма организации НИОКР, которая обеспечивает интеграцию науки, образования, производства и бизнеса. Создается система с центром - информационной базы данных. Интеллектуальная организация должна обладать ценными активами, интеллектуальным капиталом, специалистами компании, обладающими уникальными знаниями и опытом, их разработками и технологиями, позволяющими иметь конкурентное преимущество на рынке [3]. Под базами знаний понимает совокупность фактов и правил вывода, допускающих логический вывод и осмысленную обработку информации. Информационнаяинфраструктураиееинтерактивная составляющая является одними из важнейших звеньев системы поддержки инновационной деятельности. Базы данных предприятия содержат структурированную информацию о производстве, технологиях, оборудовании, рыночной ситуации

Успех высокотехнологичных предприятий измеряется рыночной долей, на которых позиционирует предприятие, уникальностью его технологий, ценностным отношением потребителей рынка к инновационной продукции предприятий. Формы приобретения РИД в практике транснациональной инновационной деятельности следующие: лицензирование, прямые иностранные инвестиции, совместные предприятия, слияние, промышленно – производственные зоны и другие.

Для успешного продвижения необходимо формировать новые структуры системного взаимодействия: а) на федеральном уровне - Центры, содействующие коммерциализации; б) Управление НИОКР; в)Структуры привлечения венчурных инвесторов в высокотехнологичные разработки; г) Центры учета и идентификации интеллектуальной собственности; д) Центры стратегического развития; е) Информационно-аналитический Центр, предоставляющий информацию о новых разработках на глобальном уровне.

Самыми распространенными формами (каналами) продвижения высокотехнологичного продукта являются[3]:

- использование прав на интеллектуальную собственность (передача исключительных прав по лицензионному договору, договору франчайзинга или договору отчуждения);
- создание новых предприятий, деятельность которых основывается на использовании разработанной технологии или результатах НИОКР;
- коммерческие контракты на реализацию НИОКР.

Каждая научно-техническая разработка по-своему уникальна, а соответственно формы выхода на рынок могут быть самыми разнообразными. В конечном счете, результатом коммерциализации инновационного продукта, как правило, является либо объект интеллектуальной собственности, подлежащий продаже, либо ее практическая реализация в каком-либо продукте, товаре или услуге. Однако, возможны и сочетания этих форм.

Например, при продаже технологии независимой компании продавец может также получить долю в ее акционерном капитале и произвести поставку своего оборудования другим независимым фирмам. Возможны и многие другие комбинации передачи технологий, форма которых зависит от особенностей высокотехнологичной продукции и конъюнктуры рынка.

В настоящий момент в Российской Федерациинет устоявшейся и законодательно оформленной классификации методов передачи технологий. В систематике, принятой ЮНКТАД

(UnitedNationsConferenceforTradingand-Development—конференция ООН по торговле и развитию),выделяются следующие формы возможных сделок при обмене высокотехнологичных разработок[4]:

- продажа или передача по лицензии всех форм промышленной собственности (при этом товарные знаки и фирменные наименования могут не являться объектами сделки);
- передача «ноу-хау» (секрета производства) и необходимых сведений для его использования в коммерческой деятельности;

- передача определенных технологических знаний (например, таких как функциональная схема эксплуатации оборудования) или выполнение проектов по внедрению технологий в производство «под ключ», оказание проектно-конструкторских услуг;
- технологические консультации (консалтинговые услуги), предоставление знаний для определенных видов деятельности, необходимых для эксплуатации оборудования или создания промежуточных товаров или сырьевых компонентов;
- соглашения о технологическом сотрудничестве (например, договор о научно-технической кооперации, предоставление административных и управленческих услуг).

Кроме перечисленных форм из номенклатуры ЮНКТАД в литературе описаны и многие другие методы передачи технологий, при этом обмен технологиями может проводиться как коммерческим путем, так и не коммерческим:

- научно-технические публикации и специализированная литература;
- информационные массивы и компьютерные банки данных;
- патенты на изобретения, полезные модели или опытные образцы;
- материалы конференций, презентаций, симпозиумов, семинаров;
- обучение, стажировки и практики студентов, аспирантов, ученых и специалистов;
- перекрестное лицензирование технологий или их отдельных компонентов на паритетной основе;
- миграция ученых и специалистов с необходимым набором знаний в другие организации («утечка мозгов»);
- передача технологии в материализованном виде, то есть продажа оборудования (станков, агрегатов, технологических линий и т.п.);
- модернизация предприятий и производств, инжиниринг;
- создание инновационных предприятий для производства и последующей продажи готовых товаров или услуг.

Комбинации методов, которые применяются при продвижении высокотехнологичной разработки на рынок, могут существенно меняться в зависимости от масштаба области реализации и применения разработанных технологий, а так же финансовых и инвестиционных возможностей организации, обладающей правами на технологии.

Целесообразность использования тех или иных методик во многом зависит от специфики ведения бизнеса и стратегии организации, внедряющей высокотехнологичные разработки.

Например, предприятия-изготовители промышленного оборудования и техники в сложившихся экономических условиях направлены на технологическую модернизацию и повышение конкурентоспособности. Как следствие, заинтересованы выйти на рынки соседних регионов, но затраты на логистику по доставке их продукции могут быть неоправданными. В этом случае производителям может быть выгоднее продать лицензию предприятию из соседнего региона (с возможным входом в состав его акционеров или без него) и оказывать ему в дальнейшем консультативно-технологические услуги, чем самому тратиться на открытие производства и найм персонала на отдаленной территории[5].

В настоящий момент описано достаточно много разнообразных стратегий для продвижения высокотехнологичной продукции на рынок. Выбор их оптимальной комбинации выполняется менеджментом компании исходя из коммерческих интересов и целей предприятия. Все инновационные стратегии можно разделить на две большие группы.

Первая группа стратегий ориентирована на предприятия, которые проводят научные исследования и создают инновационные технологические разработки. Такие стратегии позволяют установить оптимальные методы инвестирования в НИОКР, характер возможного заимствования идей, а также взаимосвязи высокотехнологичных разработок с уже существующими продуктами и процессами. При отборе перспективных разработок необходимы SWOT- и PEST-анализы. На основе SWOT-анализа выявляют возможности и угрозы для технологий, на основе PEST-анализа - влияние внешней среды, а также проводят прогноз востребованности технологий.

Стратегия следования за рынком: предприятие нацелено на выпуск коммерчески наиболее рентабельной и пользующейся спросом продукции в данный промежуток времени. Стратегия выжидания лидера: характерна для крупных отраслевых предприятий-лидеров в моменты выхода на рынок новой продукции, на которую спрос еще окончательно не определен, в этом случае сначала на рынок с новой продукцией выходит малое предприятие, а в случае ее успешной реализации подключается предприятие-лидер.

Портфель инновационных стратегий предприятия может быть сформирован путем отбора ключевых факторов развития организации. Среди таких факторов можно выделить следующие: уровень применяемых технологических решений, наличие портфеля патентов, защищающих уникальную продукцию, конкурентные преимущества предприятия, ценностное отношение потребителей рынка к продукции предприятия, государственная поддержка инновационных предприятий, регулирование отрасли.

На рис.1 отражена схема отбора ценностной информации, имеющейся в базах знаний

Рис.1 Процесс отбора, анализа и использования знаний

При анализе различных сегментов мирового рынка выявляют ценностное отношение потребителей к новой продукции или технологиям. Учитывают менталитет и специфику восприятия нового товара на выбранных сегментах рынка, реакцию на ценовые параметры и требования к качеству и сервису услуг. Оценивают издержки на продвижение продукции, разрабатывают стратегии продвижения .

Выделим этапы продвижения новых разработок:

- выполнение научного проекта,
- проведение экспертизы результатов НИОКР,
- закрепление прав на интеллектуальную собственность,
- разработка бизнес-проекта,
- подбор инвесторов,
- подготовка продукции к презентации,
- продвижение на выставках-ярмарках,
- оценка рыночной стоимости разработок,
- работа со специалистами центра коммерциализации технологий,
- использование интернет-инструментов для продвижения.

Продвижением инновационных проектов должны заниматься специальные эксперты-аналитики и маркетологи инноваций. В Европе таких специалистов именуют «драйверами» инновационных проектов, которые имеют соответствующие знания и опыт. В России также необходимо подготавливать таких специалистов. Требуется и создание рабочей группы по международному сотрудничеству в сфере инновационных технологий из числа представителей федеральных органов исполнительной власти.

Технологическая политика государства – это комплекс мероприятий по созданию, адаптации и распространению в производстве новых технологий, который обусловливает появление на рынке новых товаров, рост производственной эффективности предприятий. Для ее эффективного проведения необходимо создание информационно технологического пространства – информационной базы данных по научным и технологическим достижениям. Формирование механизмов продвижения российских товаров и услуг, уникальных разработок на мировые рынки должно стать важнейшим шагом в экономическом развитии страны. Для технологического лидерства предприятиям необходимо осуществлять: интенсивные исследования, предшествующие технологическим разработкам; создание результатов интеллектуальной деятельности и их прогнозную оценку, высококлассный сервис при продажах продукции.

Результаты

Развитие технологий, поддержка высокотехнологичных компаний, выстраивание благоприятной среды для стартапов, быстрое внедрение и коммерциализация новых разработок являются необходимыми факторами для создания конкурентоспособной экономики страны.

В работе показано, что эффективными механизмами создания и продвижения результатов интеллектуальной деятельности является развитая инновационная инфраструктура, включающая центры развития, центры коммерциализации, патентные стратегии и участие в международных ассоциациях. Предложена и обоснована базисная стратегия развития инновационных предприятий с учетом оценки интеллектуального капитала, продвижения на рынок и сохранение устойчивого положения в течение жизненного цикла развития технологии, продукции и самого предприятия.

Заключение.

Выбор оптимальной модели при продвижении разработанной технологии выполняется руководством организации в зависимости от ее целей, миссии, возможностей и области коммерческих интересов. Реальные пути выхода инновации на рынок в новых условиях интенсивного развития - это оформление технологии как перспективного инновационного бизнес-проекта, отслеживание благоприятных ситуаций в наукоемком секторе производства, использование услуг бизнес-инкубаторов. Окончательный выбор методов и определение стратегии должны проводиться комплексно с учетом организационно-экономических и научно-технических факторов по результатам проведения комплексной оценки привлекательности научно-технической разработки группой квалифицированных экспертов и ценностного отношения потребителей рынка к предлагаемой продукции.

Список литературы

1. «Об утверждении Перечня инновационной, высокотехнологичной продукции и технологий» (в редакции приказа Департамента от 15.03.2019 № П-18-12-60/9 «О внесении изменений в приказ Департамента от 9 ноября 2018 г. № П-18-12-18/8»).

2. Устинова Л.Н. Технология продвижения новых разработок // Креативная экономика. – 2009. – Том 3. – № 10. – С. 56-60
3. Мухопад В.И. Коммерциализация интеллектуальной собственности.-М:Магистр:ИНФРА-М, 2012.-512с.
4. ЮНКТАД (United Nations ConferenceforTradingand Development)—конференция ООН по торговле и развитию
5. Устинова Л.Н.«Цифровые технологии в управлении интеллектуальными ресурсами предприятий/ коллективная. Монография СПбГПУ«Цифровые технологии в управлении инновационной деятельностью предприятий» INDYSTRY-2017 (сборник трудов в базе РИНЦ), 2017.
6. Татаринов В. В. Продвижение наукоемких технологий на рынок // Бизнес-образование в экономике знаний Иркутский гос. университет No 1 за 2017.

Подписано в печать 15.02.2018
Формат 60x90/8 Бумага офсетная. Гарнитура Gilroy.
Усл. печ. л. 7,4. Тираж 900 экз. Заказ 016 от 14.06.2019.
Издательство:
ООО «Фабрика галтовочного оборудования и технологий
– инжиниринг» («ФАГОТ-ИНЖИНИРИНГ»),
107241, г. Москва, Черницынский проезд, д. 3.
Отпечатано в типографии
ООО «Белый ветер»
115054, Москва, ул. Щипок, д. 28.