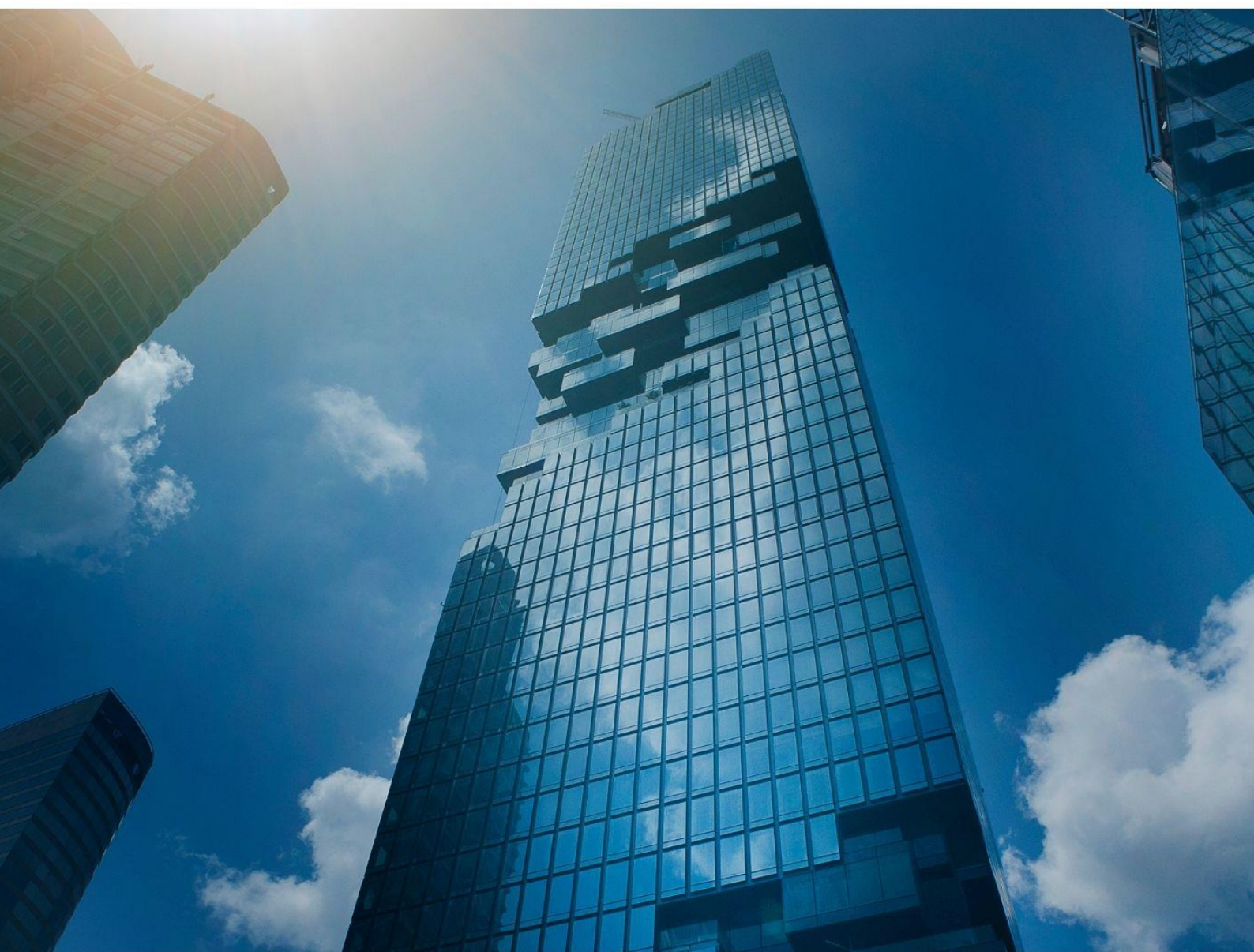


ЭКОНОМИЧЕСКИЕ ИССЛЕДОВАНИЯ И РАЗРАБОТКИ

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОННЫЙ ЖУРНАЛ



EDRJ.RU

ISSN 2542-0208

Экономическая теория
Экономика, организация и управление предприятиями,
отраслями, комплексами
Управление инновациями
Экономика и управление в образовании
Государственное управление
Региональная экономика
Мировая экономика
Логистика

**НАУЧНАЯ ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ
ПРОФЕССИОНАЛЬНАЯ НАУКА**

**ЭКОНОМИЧЕСКИЕ ИССЛЕДОВАНИЯ И
РАЗРАБОТКИ**

**НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ЭЛЕКТРОННЫЙ ЖУРНАЛ**

№ 9/2021

www.edrj.ru

Нижний Новгород 2021

УДК 33
ББК 65
Э 401

Экономические исследования и разработки: научно-исследовательский электронный журнал. Нижний Новгород: НОО «Профессиональная наука» – №9– 2021. – 94 с.

DOI 10.54092/25420208_2021_9

ISSN 2542-0208

Статьи журнала содержат информацию, где обсуждаются наиболее актуальные проблемы современного экономического развития и результаты фундаментальных исследований в различных областях знаний экономики и управления.

Журнал предназначен для научных и педагогических работников, преподавателей, аспирантов, магистрантов и студентов с целью использования в научной работе и учебной деятельности.

Все включенные в журнал статьи прошли научное рецензирование и опубликованы в том виде, в котором они были представлены авторами. За содержание статей ответственность несут авторы.

Информация об опубликованных статьях предоставлена в систему Российского индекса научного цитирования – **РИНЦ** по договору No 685-10/2015.

Электронная версия журнала находится в свободном доступе на сайте www.edrj.ru

УДК 33
ББК 65

Редакционная коллегия:

Главный редактор – **Краснова Наталья Александровна**, кандидат экономических наук, доцент, руководитель НОО «Профессиональная наука» (mail@scipro.ru)

Балашова Раиса Ивановна – доктор экономических наук, доцент, профессор кафедры “Экономика предприятия” Донецкого национального технического университета.

Глебова Анна Геннадьевна – доктор экономических наук, профессор экономики и управления предприятием ФГБОУ ВО «Тверской государственный технический университет», член Новой экономической ассоциации. Эксперт научных направлений – антикризисное управление и банкротство, экономика предприятия и предпринимательства, управление.

Кожин Владимир Александрович – заслуженный экономист РФ, доктор экономических наук, профессор кафедры организации и экономики строительства Нижегородского государственного архитектурно-строительного университета. Эксперт научных направлений – финансы, бюджетирование, экономика предприятия, экономика строительства.

Мазин Александр Леонидович – доктор экономических наук, профессор кафедры экономической теории Нижегородского института управления, филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации. Эксперт научных направлений: экономика труда, экономическая теория.

Бикеева Марина Викторовна – кандидат экономических наук, доцент кафедры статистики, эконометрики и информационных технологий в управлении Национального исследовательского Мордовского государственного университет им. Н.П. Огарёва. Эксперт научных направлений: социальная ответственность бизнеса, эконометрика, статистика.

Лаврентьева Марина Анатольевна – кандидат экономических наук, старший преподаватель кафедры социальной медицины и организации здравоохранения. ФГБОУ ВО “Нижегородская государственная медицинская академия” Министерства здравоохранения Российской Федерации. Эксперт научных направлений: учет, анализ, аудит, экономическая теория, экономика труда.

Тиндова Мария Геннадьевна – кандидат экономических наук; доцент кафедры прикладной математики и информатики (Саратовский социально-экономический институт (филиал) ФБГОУ ВПО РЭУ им. Плеханова). В полномочия входят организация и/или проведение экспертной оценки статей по проблемам экономико-математического моделирования.

Шагалова Татьяна Владимировна – кандидат экономических наук, доцент кафедры менеджмента и государственного управления ННГУ им. Н.И. Лобачевского. Эксперт научных направлений: бюджетирование, мировая экономика, ценообразование, экономика предприятия, инновационный менеджмент.

Материалы печатаются с оригиналов, поданных в оргкомитет, ответственность за достоверность информации несут авторы статей

© НОО Профессиональная наука, 2015-2021

Оглавление

РЕКРЕАЦИЯ И ТУРИЗМ	6
Гаврилова К.С., Сосункевич В.О. Направления туристской политики в Японии: современные реалии	6
СТАНДАРТИЗАЦИЯ И УПРАВЛЕНИЕ КАЧЕСТВОМ	12
Платонова С.Д., Оськин В.С. Основные принципы защиты персональных данных в автоматизированных информационных системах коммерческих предприятий на территории Российской Федерации	12
ФИНАНСЫ, ДЕНЕЖНОЕ ОБРАЩЕНИЕ И КРЕДИТ	52
Панова А.Ю., Мамедова А.Р. Потребительское кредитование в России в период пандемии	52
ЭКОНОМИКА ПРЕДПРИНИМАТЕЛЬСТВА	60
Балашова Р.И., Гречина И.В., Леонова Л.А. Эффективность сферы услуг региональной экономики: субъекты предпринимательства, инновации, территория	60
ЭКОНОМИКА ПРИРОДОПОЛЬЗОВАНИЯ	68
Энхтүвшин Л., Ганчимэг Ж. Некоторые вопросы по планированию, контролю и анализу данных открытых рудников	68
ЭКОНОМИКА ТРУДА	83
Кудрявцева М.В. Лидерство руководителей как фактор повышения эффективности деятельности современных компаний	83
ЭКОНОМИЧЕСКАЯ ТЕОРИЯ	88
Луговая Н. Г. Страхование, новые тренды и динамика развития	88

Рекреация и туризм

УДК 33

Гаврилова К.С., Сосункевич В.О. Направления туристской политики в Японии: современные реалии

Directions of tourism policy in Japan: modern realities

Гаврилова Каринэ Самвеловна,

старший преподаватель кафедры региональной экономики и природопользования,

Санкт-Петербургский государственный экономический университет

Сосункевич Варвара Олеговна,

студентка направления «Зарубежное регионоведение»,
профиль – Азиатско-Тихоокеанский регион,

Санкт-Петербургский государственный экономический университет

Gavrilova Karine Samvelovna,

Senior lecturer, the Department of Regional Economics
and Nature Management,

Saint-Petersburg State University of Economics

Sosunkevich Varvara Olegovna,

Student, Specialization «Foreign Regional Studies» («Asian-Pacific area»)

Saint-Petersburg State University of Economics

Аннотация. Статья посвящена анализу реализации Национального плана по развитию туризма, утвержденного Кабинетом Премьер-Министра Синдзо Абэ в 2012 г. Интерес представляет его успешная реализация в допандемийный период. Авторы рассматривают вклад туристской отрасли в экономику страны, а также, используя метод SWOT-анализа, выявляют потенциал ее развития. Особое внимание в статье уделяется состоянию данного сектора в настоящее время.

Ключевые слова: Япония, туризм, туристский сектор экономики, SWOT-анализ, проект «Go to travel», въездной туризм, внутренний туризм

Abstract. The article is devoted to the analysis of the implementation of the National Plan for Tourism Development, approved by the Cabinet of Prime Minister Shinzo Abe in 2012. Its successful implementation in the pre-pandemic period is of interest. The authors examine the contribution of the tourism industry to the country's economy, and also, using the SWOT analysis method, identify the potential for its development. The article focuses on the current state of this sector.

Key words: Japan, tourism, tourism sector of the economy, SWOT analysis, «Go to travel» project, inbound tourism, domestic tourism

DOI 10.54092/25420208_2021_9_6

Рецензент: Дудкина Ольга Владимировна, кандидат социологических наук, доцент.
Донской государственный технический университет (ДГТУ), г. Ростов-на-Дону, Факультет
«Сервис и туризм», кафедра «Сервис, туризм и индустрия гостеприимства»

Правительство Синдзо Абэ поставило перед собой задачу превратить Японию в мировой туристский центр. Это стало особенно актуально в связи с выбором Токио в

качестве места проведения Олимпийских игр 2020. В 2013 г. была опубликована утвержденная ранее стратегия развития туристской отрасли страны. [4] В соответствии с ней к 2030 г. ежегодное количество иностранных туристов, посещающих страну, должно достигнуть отметки 30 млн чел. Активная политика по продвижению японского туристского бренда показала положительные результаты в допандемийный период (см. рис. 1).



Рисунок 1. Темпы прироста численности иностранных туристов, прибывших в Японию в период с 2012 по 2020 гг.

В 2019 г. численность иностранных туристов, прибывших в Японию, составила 31,88 млн чел. [10] Общий вклад отрасли в структуру ВВП в 2019 г. составил 7,7%. [5]

Правительством страны проводилась последовательная политика, направленная на упрощение въезда в страну для иностранных граждан, на формирование гостеприимной и комфортной среды внутри страны, а также на продвижение туристского бренда Японии за рубежом. В частности, на сегодняшний день граждане 68 стран могут посещать Японию без оформления визовых документов с туристскими целями (ограничивается срок пребывания на территории страны до 90 дней). [2] С 01.01.2017 г. был упрощен визовый режим и для граждан России: при оформлении документов на выезд перестали требовать приглашение принимающей стороны, а также взимать консульский сбор. [1]

К формированию «дружелюбной среды», в соответствии с принятой органами власти «дорожной картой», были отнесены следующие меры: развитие внутренней

транспортной инфраструктуры, увеличение численности мест размещения (отели разных категорий, хостелы и т.д.), транслитерация надписей и указательных знаков на улицах городов и поселений, распространение различных справочных материалов на иностранных языках, расширение бесплатной публичной сети WiFi, увеличение числа магазинов беспошлинной торговли (duty free). [4]

Помимо означенных выше пунктов проводилась широкомасштабная рекламная кампания по продвижению туристского бренда Японии на международный рынок. Привлечь внимание аудитории к этой дестинации удалось в том числе за счет использования современного медиапространства. Одно лишь видео о достопримечательностях Японии «Enjoy my Japan», размещенное на сайте youtube.com, было просмотрено почти 60 млн раз. [7] Функционирование официальных туристских сайтов позволяет узнать всю необходимую информацию о стране.

Для финансовой поддержки отрасли с 07.02.2019 г. в Японии был введен туристский налог, распространяющийся как на иностранных граждан, так и на местных туристов. [3]

Несмотря на значительное число мер по привлечению в страну иностранных туристов, внутренний туризм в стране развит гораздо сильнее. В том же году количество граждан Японии, занимавшихся туризмом внутри страны, составило 587,1 млн чел. [10] Вклад внутреннего и въездного туризма оказывает крайне неравномерное влияние на формирование ВВП страны – 81% и 19% соответственно. [10] Расходы иностранных туристов в 2019 г. составили 4,81 млрд японских йен. Расходы внутренних туристов в том же году оценивались в 21,9 млрд японских йен. [10]

Тем не менее, несмотря на инициативу бывшего премьер-министра превратить Японию в ведущий мировой туристский центр, на сегодняшний день реализовать ее будет крайне затруднительно. В 2020 г. в условиях нестабильной эпидемиологической обстановки существенно сократился приток иностранных туристов и составил всего 4,12 млн чел. (туристский поток сократился почти в 8 раз). [10] Безусловно, внутренний туризм также пострадал от введенных ограничений, однако количество туристов сократилось всего лишь в 2 раза и составило 293,41 млн чел. [10]

Безусловно, текущая неблагоприятная ситуация рассматривается экспертами как временная. Грамотно разработанная стратегия вывода отрасли из кризисного состояния позволит изменить ситуацию в лучшую сторону. Для выявления потенциала развития туристской отрасли обратимся к методу SWOT-анализа.

Таблица 1

SWOT-анализ туристской отрасли Японии

Сильные стороны	Слабые стороны
• расположение страны в центре Азиатско-Тихоокеанского региона • разнообразие климатических условий • разнообразие природных ландшафтов • богатое историческое и культурное наследие • разнообразие реализуемых событийных мероприятий • высокий уровень экономического развития • развитый транспортно-логистический комплекс • развитая туристская инфраструктура • наличие известного на международном рынке туристского бренда	• островное расположение государства • расположение в сейсмически активной зоне • удаленность территории страны от большинства развитых стран мира • удаленность от ключевых туристских потоков • достаточно высокая стоимость японской иены • неблагоприятные климатические условия (высокая влажность, знойное лето) • языковой барьер у местного населения • существенное отличие культурных ценностей, присущих японской нации • неблагоприятная экологическая обстановка в крупных городах
Возможности	Угрозы
• дальнейшая популяризация Японии как туристской дестинации • проведение мероприятий международного значения (пример: Олимпийские игры) • дальнейшая реализация «дорожной карты» по развитию туристского сектора страны и формирования дружелюбной среды для иностранных туристов • развитие экотуризма за счет популяризации существующих в стране особо охраняемых природных территорий • увеличение туристского потока за счет упрощения визовых требований • дальнейшее стимулирование развития внутреннего туризма • наличие потенциала для привлечения инвестиций в туристский сектор страны • формирование туров, включающих посещение нескольких туристских дестинаций (соседних стран)	• природные катаклизмы • политические конфликты • дальнейшая дестабилизация эпидемиологической обстановки • высокая стоимость транспортных расходов • конкуренция со стороны соседних стран АТР • дальнейшая дестабилизация экономической обстановки в мире

Из перечисленных выше угроз наиболее ощутимой на сегодняшний день является нестабильная эпидемиологическая обстановка. В 2020 г. правительством страны было принято решение о дальнейшем развитии внутреннего туризма. За реализацию проекта «Go to travel», финансирование которого оценивается в 1,7 трлн иен, отвечает Национальная туристская организация Японии. [6] Срок реализации программы – до конца сезона 2021 г.

Данная система включает в себя предоставление скидки на проживание (до 35%) и получение купонов в размере 15% от затрат на тур. К примеру, турист бронирует отель,

стоимость пребывания в котором оценивается в 40 тыс. иен. Он получает скидку и оплачивает 65% стоимости, то есть 26 тыс. иен. При этом турист также получает купон на 6 тыс. иен, составляющий 15% первоначальной стоимости.

Купоны могут быть использованы для оплаты покупок в магазинах и заказов в ресторанах, принимающих участие в акции, а также для покрытия транспортных расходов в границах посещаемой префектуры. Использовать полученные купоны можно исключительно в период поездки. Обналичивание средств не допускается.

При этом устанавливаются верхние и нижние допустимые границы предоставляемых скидок – не менее 7 тыс. иен и не более 13 тыс. иен. Стоимостная градация купонов находится в диапазоне от 3 тыс. до 7 тыс. иен. Особо подчеркивается тот факт, что данная акция распространяется исключительно на граждан Японии. Временно пребывающие на территории страны иностранные граждане не могут претендовать на участие в ней. В территориальном отношении проект охватывает все префектуры страны. [8]

Национальный базовый план по развитию туризма основывается на Законодательном акте №117 «О развитии туризма» от 2006 г. Стратегия была утверждена правительством в 2012 г. [9] Обозначенная в ней цель была успешно достигнута в допандемийный период благодаря грамотно разработанным мерам по продвижению туристского бренда Японии на международном рынке туристских услуг, упрощению визовых процедур, формированию комфортной для туристов среды внутри страны. Тем не менее мировая пандемия COVID-19 поставила туристский сектор в кризисное положение. Границы Японии были закрыты для 100 стран мира. Поток иностранных туристов сократился в 8 раз. Оптимальным выходом из сложившейся ситуации, по мнению правительственных структур, стала реализация проекта по стимулированию внутреннего туризма. Данная стратегия позволила поддержать менее популярные среди иностранцев туристские центры, охватив все регионы страны.

Библиографический список

1. Виза в Японию // Туристский портал [Электронный ресурс]. Режим доступа: <https://www.tourister.ru/world/asia/japan/publications/1078>
2. Официальный туристский портал Японии [Электронный ресурс]. Режим доступа: <https://www.visasjapan.com>
3. Политика Японии в области развития туризма и новый туристический налог // Общероссийская общественная организация «Общество «Россия – Япония» [Электронный ресурс]. Режим доступа: <https://russiajapansociety.ru/?p=8764>

4. Томоми Нагаи Серьезный подход к международному туризму // Современный взгляд на Японию [Электронный ресурс]. Режим доступа: <https://www.nippon.com/ru/in-depth/a03703/?pnum=2>
5. Япония – Туризм, общий вклад в ВВП // Мировой атлас данных [Электронный ресурс]. Режим доступа: <https://knoema.ru/atlas/>
6. Япония будет субсидировать туристические поездки только для жителей страны // Интерфакс [Электронный ресурс]. Режим доступа: <https://tourism.interfax.ru/ru/news/articles/70268/>
7. Enjoy my Japan // YouTube.com [Электронный ресурс]. Режим доступа: <https://www.youtube.com/watch?v=Z8EGy3nhpNI>
8. Go to travel // Официальный портал проекта «Go to travel» [Электронный ресурс]. Режим доступа: <https://goto.jata-net.or.jp/>
9. The Tourism Nation Promotion Basic Plan // Официальный сайт японского агентства по туризму [Электронный ресурс]. Режим доступа: <https://www.mlit.go.jp/kankocho/en/kankorikkoku/kihonkeikaku.html>
10. Travel and tourism in Japan // Статистический портал Statista [Электронный ресурс]. Режим доступа: <https://www.statista.com/study/57443/travel-and-tourism-in-japan/>

Стандартизация и управление качеством

УДК 33

Платонова С.Д., Оськин В.С. Основные принципы защиты персональных данных в автоматизированных информационных системах коммерческих предприятий на территории Российской Федерации

Basic principles of personal data protection in automated information systems of commercial enterprises on the territory of the Russian Federation

Платонова Софья Дмитриевна
Оськин Владимир Сергеевич

1. Студентка кафедры радиофизики и радиоэлектроники направления «Информационная безопасность» Иркутского государственного университета
2. Директор ООО «ТехноСтиль»

Platonova Sofia Dmitrievna
Oskin Vladimir Sergeevich

1. Irkutsk State University, Department of radio physics and radio electronics, Information security
2. Director ООО «TechnoStil»

Аннотация. В связи с развитием компьютеризации всех сфер жизнедеятельности человека в 21 веке особенно актуален вопрос защиты персональных данных пользователей. Основная цель исследования-определение основных принципов защиты персональных данных в автоматизированных информационных системах коммерческих предприятий на территории Российской Федерации. В качестве методов защиты в статье описываются этапы классификации коммерческих предприятий для последующего определения потенциальной модели угрозы и составления плана защиты.

Ключевые слова: персональные данные, коммерческое предприятие, классификация автоматизированных систем, модель угроз, методы защиты.

Abstract. In connection with the development of computerization of all spheres of human activity in the 21st century, the issue of protecting users' personal data is especially relevant. The main purpose of the study is to determine the basic principles of personal data protection in automated information systems of commercial enterprises on the territory of the Russian Federation. As methods of protection, the article describes the stages of classification of commercial enterprises for the subsequent determination of a potential threat model and the preparation of a protection plan.

Keywords: personal data, commercial enterprise, classification of automated systems, threat model, protection methods.

DOI 10.54092/25420208_2021_9_12

Рецензент: Бессарабов Владислав Олегович - Кандидат экономических наук. ГО ВПО «ДонНУЭТ имени Михаила Туган-Барановского»

Введение

Для современной постиндустриальной эпохи характерны непрерывные и развивающиеся процессы информатизации и компьютеризации общества. Активно развиваются сферы услуг, происходит глобализация экономики и единицей товара становятся знания. При такой ситуации в мире, информация, обладая высокой материальной ценностью и впоследствии представляя собой главный объект интересов злоумышленников, требует определенных стандартов по обеспечению защиты от несанкционированного доступа.

Информационно-вычислительные системы различного рода, электронный документооборот, электронные системы оплаты услуг, электронная почта, электронные базы данных и многие другие технические средства внедрились во все сферы деятельности современного человека: в управление, экономику, образование, медицину, досуг. Для упрощения рабочего процесса государственные органы управления, а также частные предприятия крупного, среднего и малого бизнеса вынуждены использовать автоматизированные информационные системы. Именно поэтому, в связи с увеличением влияния информационных технологий на коммерческую среду, проблема защиты информации на предприятии является крайне актуальной и нуждается в особом внимании со стороны разработчиков требований безопасности.

Считается что тема защиты информации в организации особенно сложна для освоения и понимая, по причине того, что она располагается на стыке двух фундаментально разных отраслей: юриспруденции и технологий. С этим высказыванием трудно не согласиться, в данной работе отрасль юриспруденции представляют собой федеральные законы, акты, приказы, постановления, внутренние протоколы, правила организации и другие организационно-правовые меры. Технологией и техническими средствами, в данном случае, являются все электронно-механическое приспособления и программы, входящие в автоматизированную информационную систему и применяемые для решения различных задач по защите информации. Несмотря на обширность и труднодоступность информации в рамках изучаемого вопроса, исследование мер безопасности на предприятии представляется возможным для обоих аспектов защиты информации в совокупности.

Основной целью работы является изучение организационных и технических мер защиты персональных данных в автоматизированной информационной системе на предприятии коммерческого типа.

Для достижения поставленной цели необходимо решить ряд задач:

1. Изучение текущего законодательства Российской Федерации об информационных системах и работе с персональными данными.

2. Классификация организации по классу защищенности, необходимая для дальнейшего разбития системы по разным параметрам и работы с ней в рамках класса.
3. Формулировка требований защищенности для данного класса.
4. Составление модели потенциальных угроз в автоматизированной системе предприятия.
5. Определение методов защиты информации для выбранной модели угроз.

Объекты и методы исследования

Объектом исследования работы служит автоматизированная система, содержащая и обрабатывающая персональные данные. Предметом исследования в данном случае являются особенности организации процесса безопасности в автоматизированной системе коммерческого предприятия.

К методам исследования в представленной работе относятся:

1. Анализ нижеперечисленной документации, соответствующей по уровню к требованиям, предъявляемым для автоматизированных информационных систем:
 - ФЗ РФ №152 «О персональных данных» от 27 июля 2006 г.
 - Постановление Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г.
 - Приказ №21 ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г.
 - Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гос. тех. комиссии при Президенте РФ от 30 марта 1992 г.
 - Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России от 11 февраля 2014 г.
 - Приказ №17 ФСТЭК «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г.

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена зам. директора ФСТЭК России от 15 февраля 2008 г.
- 2. Свободный опрос руководства и сотрудников предприятия об основных бизнес-процессах организации.
- 3. Моделирование потенциальных методов угроз и защиты.

Глава 1. Классификация

В настоящее время классификация всех автоматизированных систем (АС), располагающихся на частных предприятиях, осуществляется на основании руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.).

Основными этапами классификации автоматизированной системы, согласно вышеупомянутому документу, являются:

1. разработка и анализ исходных данных АС;
2. выявление основных признаков АС, необходимых для классификации;
3. сравнение выявленных признаков АС с классифицируемыми;
4. присвоение АС соответствующего класса защиты информации от несанкционированного доступа (НСД).

К числу определяющих признаков, по которым производится группировка автоматизированной системы в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на допуск к конфиденциальной информации;
- режим обработки данных в АС: коллективный или индивидуальный.

В заданной автоматизированной информационной системе не содержится информация различных уровней конфиденциальности. Различается уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации: не все сотрудники компании имеют доступ ко всем техническим средствам, базам данных и документам. Также в автоматизированной системе происходит коллективный режим обработки данных.

Согласно вышеописанным признакам автоматизированную систему определяем к первой группе. Первая группа имеет следующие характеристики:

- группа включает многопользовательские АС, в которых одновременно обрабатывается или хранится информация разных уровней конфиденциальности;
- не все пользователи имеют право доступа ко всей информации АС;
- группа содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А.

В автоматизированной системе предприятия обрабатывается служебная информация, коммерческая тайна, персональные данные и информация не выше грифа «секретно» поэтому АС определяется возможными классами: 1В, 1Г или 1Д.

Для более точной классификации АС на предприятии необходимо изучить основные принципы работы системы и сравнить их с критериями, относящимися к предполагаемым классам. В ходе опроса руководителя и сотрудников организации, а также детального анализа системы были выявлены требования, предъявляемые к системе, представленные далее, в таблице приложения №1. В этой же таблице представлены три предполагаемых класса и требования, предъявляемые к этим классам.

На основании полученных в результате опроса и представленных в приложении 1 требований к автоматизированной информационной системе и её подсистемам, АИС можно отнести к классу 1В.

1.2. Требования к классу защищенности 1В

К автоматизированной системе класса защищенности 1В и её подсистемам для обеспечения высокого уровня безопасности на всех этапах ее работы предъявляются различные требования. Согласно руководящему документу «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденному решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года эти требования относятся к подсистеме управления доступом, подсистеме регистрации и учета и к подсистеме обеспечения целостности.

Требования к подсистеме управления доступом:

1. должна осуществляться идентификация субъектов доступа при входе в систему по идентификатору и паролю длиной не менее шести буквенно-цифровых символов;
2. должна осуществляться идентификация терминалов, каналов связи, ЭВМ и её узлов сети и внешних устройств по логическим именам или адресам;

3. должна осуществляться идентификация программ, каталогов, файлов, записей, полей записей по именам;
4. должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
5. должно осуществляться управление потоками информации с помощью меток конфиденциальности. Уровень конфиденциальности накопителей не ниже 4-го уровня.

Требования к подсистеме регистрации и учета:

1. должна осуществляться регистрация входа и выхода субъектов доступа в систему и из нее, либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная — несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке;

2. должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача сопровождается автоматической маркировкой каждой страницы документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества страниц. В параметрах регистрации указываются:

- дата и время выдачи (обращение к подсистеме вывода);
- спецификация устройства выдачи (логическое имя или номер внешнего устройства);
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;
- объем фактически выданного документа (количество страниц, копий) и результат выдачи: успешный (весь объем), неуспешный;

3. должна осуществляться регистрация запуска или завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный);

4. должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
- вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

5. должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная — несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта (логическое имя или номер);
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
- вид запрашиваемой операции (чтение, запись, монтирование, захват);

6. должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего изменения;

7. должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка отражает уровень конфиденциальности объекта;
8. должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал или учетную карточку;
9. учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
10. должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;
11. должна осуществляться очистка (обнуление или обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;
12. должна осуществляться сигнализация попыток нарушения защиты.
Требования к подсистеме обеспечения целостности:
 1. должна быть обеспечена целостность программных средств защиты информации (СЗИ) НСД, а также неизменность программной среды. При этом:
 - целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
 - целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке или хранении защищаемой информации;
 2. должна осуществляться физическая охрана средств вычислительной техники (СВТ), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
 3. должен быть предусмотрен администратор или служба защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;
 4. должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год;

5. должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД, их периодическое обновление и контроль работоспособности;
6. должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.
7. При работе с автоматизированной системой класса защищенности 1В необходимо использовать сертифицированные средства вычислительной техники не ниже 4 класса защищенности.

Глава 2. Модель угроз

2.1. Общий список потенциальных моделей угроз

На основе опроса сотрудников и руководителя компании об организационной деятельности, программно-аппаратного анализа автоматизированной системы, визуального анализа офисных помещений и согласно документу ФСТЭК России «Базовая модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена» от 15 февраля 2008 года, для выбранной автоматизированной системы класса 1В выделяют следующие угрозы:

- угрозы утечки информации по техническим каналам:
 - угрозы утечки акустической (речевой) информации;
 - угрозы утечки видовой информации.
- угрозы несанкционированного доступа к информации в информационной системе персональных данных:
 - источники угроз несанкционированного доступа в информационной системе персональных данных;
 - уязвимости информационной системы персональных данных;
 - уязвимости системного программного обеспечения;
 - уязвимости прикладного программного обеспечения.
 - угрозы с использованием протоколов межсетевого взаимодействия;
 - угрозы программно-математических воздействий;

- угрозы безопасности персональных данных, обрабатываемых в автоматизированных рабочих местах, имеющих подключение к сетям связи общего пользования или сетям международного информационного обмена.

2.2. Угрозы утечки информации по техническим каналам

Согласно Федеральной службе по техническому и экспортному контролю, основными элементами описания угроз утечки информации по техническим каналам (ТКУИ) являются: источник угрозы, среда распространения информативного сигнала и носитель защищаемой информации.

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к информационной системе персональных данных (ИСПДн), зарубежные спецслужбы или организации (конкурирующие или террористические), криминальные группировки, перехватывающие информацию с использованием технических средств регистрации или приема.

Среда распространения информативного сигнала — это физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Среда распространения может быть как однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований).

Носителем персональных данных (ПДн) является пользователь информационной системы персональных данных, осуществляющий голосовой ввод данных в систему, акустическая система ИСПДн, воспроизводящая ПДн, а также технические средства ИСПДн и вспомогательные технические средства и системы (ВТСС), создающие физические поля, в которых информация находит свое отражение в виде символов, сигналов, технических процессов и количественных характеристик физических величин.

К угрозам утечки информации по техническим каналам относятся угрозы утечки речевой информации и угрозы утечки видовой информации.

2.2.1. Угрозы утечки акустической информации

Возникновение угроз утечки акустической информации, содержащейся непосредственно в произносимой речи пользователя информационной системы персональных данных, при обработке этих данных в системе, обусловлено наличием функций голосового ввода информации в систему или функций воспроизведения данных акустическими средствами ИСПДн.

Перехват акустической информации в таких случаях возможен с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки персональных данных, а также в строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн.

Кроме этого, перехват речевой информации возможен с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки персональных данных, ВТСС и помещения или подключенных к каналам связи.

Перехват акустической или речевой информации может вестись:

- стационарной аппаратурой, размещаемой в близлежащих строениях с неконтролируемым пребыванием посторонних лиц;
- портативной возимой аппаратурой, размещаемой в транспортных средствах, при их нахождении рядом с этими помещениями;
- портативной носимой аппаратурой — физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них;
- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами непосредственно в служебных помещениях или в непосредственной близости от них.

2.2.2. Угрозы утечки видовой информации

Угрозы утечки видовой информации обычно реализуются за счет просмотра персональных данных с помощью оптических средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы персональных данных.

Кроме этого, просмотр или регистрация персональных данных возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Необходимым условием осуществления просмотра персональных данных является наличие прямой видимости между средством наблюдения и носителем этих данных.

Перехват персональных данных может вестись:

- стационарной аппаратурой, размещаемой в близлежащих строениях с неконтролируемым пребыванием посторонних лиц;
- портативной возимой аппаратурой, размещаемой в транспортных средствах, при их нахождении рядом с этими помещениями;
- портативной носимой аппаратурой — физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них.

2.3. Угрозы несанкционированного доступа к информации в информационной системе персональных данных

Угрозы несанкционированного доступа в ИС персональных данных с применением программно-аппаратных средств реализуются при осуществлении несанкционированного или случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) персональных данных, и включают в себя:

- угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
- угрозы создания нештатных режимов работы программно-аппаратных средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения самих данных и т.п.;
- угрозы внедрения вредоносных программ (программно-математического воздействия).

Возможны комбинированные угрозы, являющиеся сочетанием перечисленных угроз. Например, за счет внедрения различных вредоносных программ создаются условия несанкционированного доступа в операционную среду компьютера.

Состав элементов описания угроз несанкционированного доступа к информации в информационной системе персональных данных приведен на рисунке приложения 2.

2.3.1. Источники угроз несанкционированного доступа в информационной системе персональных данных

Источниками угроз несанкционированного доступа в информационной системе персональных данных могут быть:

- нарушитель;
- носитель вредоносной программы;
- аппаратная закладка.

По наличию права постоянного или разового доступа в контролируемую зону (КЗ) информационной системы нарушители делятся на два типа:

1. нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена, — внешние нарушители;
2. нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в системе, — внутренние нарушители.

Внешними нарушителями могут быть:

- разведывательные службы государств;
- криминальные структуры;
- конкурирующие организации;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования или сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла оказываются за пределами контролируемой зоны;

- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к персональным данным и контролю порядка проведения работ

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к персональным данным.

К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Ко второй категории относятся зарегистрированные пользователи информационной системы персональных данных, осуществляющие ограниченный доступ к ресурсам ИСПДн с собственного рабочего места. Доступ, аутентификация и права по доступу второй категории к некоторому подмножеству ПДн должны регламентироваться соответствующими правилами разграничения доступа.

К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным или распределенным информационным системам.

К четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента ИСПДн.

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн. Системный администратор выполняет конфигурирование и управление программным обеспечением (ПО) и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД.

К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн. Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

К седьмой категории относятся программисты-разработчики или поставщики прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на информационной системе персональных данных.

Указанные категории нарушителей учитываются при оценке возможностей реализации угрозы безопасности персональных данных. Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

- отчуждаемый носитель: дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;
- встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, — видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);
- микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с прикладной программой, файлами, с сообщениями, передаваемыми по сети, то ее носителями являются:

- пакеты передаваемых по компьютерной сети сообщений;
- файлы (текстовые, графические, исполняемые и т.д.).

2.3.2. Уязвимости информационной системы персональных данных

Уязвимость информационной системы персональных данных — это слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования программно-аппаратного обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходом ресурсов (например загрузка процессора, захват оперативной памяти);
- внедрение вредоносных программ, создающих уязвимости в программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Классификация основных уязвимостей информационной системы персональных данных приведена в рисунке приложения 3.

2.3.2.1. Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем.

При этом возможны уязвимости:

- в микропрограммах, в прошивках ПЗУ;
- в средствах операционной системы, предназначенных для управления локальными ресурсами ИСПДн (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;
- в средствах операционной системы, предназначенных для выполнения вспомогательных функций, — утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиках и т.п.), программах предоставления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.д.);
- в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, а также блокирования несанкционированно-модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и так далее. Краткая характеристика этих уязвимостей применительно к протоколам приведена в таблице приложения 4.

2.3.2.2. Уязвимости прикладного программного обеспечения

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования — это текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели и т.п.), а также системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Специальные прикладные программы — это программы, которые разрабатываются в интересах решения конкретных прикладных задач в данной информационной системе персональных данных (в том числе программные средства защиты информации, разработанные для конкретной ИСПДн).

Уязвимостями прикладного программного обеспечения являются:

- функции, относящиеся к разным прикладным программам и несовместимые между собой из-за конфликтов, связанных с распределением ресурсов системы;

- процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн и вызова штатных функций операционной системы без обнаружения изменений;
- фрагменты кода программ, введенные разработчиком, позволяющие обходить процедуры идентификации, проверки целостности и др., предусмотренные в операционной системе;
- отсутствие необходимых средств защиты (аутентификации, проверки форматов сообщений, блокирования несанкционированно-модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных и функций, в кодах программ), которые при определенных условиях приводят к сбоям функционирования систем защиты информации.

2.3.3. Угрозы с использованием протоколов межсетевого взаимодействия

Если информационная система персональных данных реализована на базе локальной или распределенной информационной системы, то в ней могут быть реализованы угрозы безопасности информации путем использования протоколов межсетевого взаимодействия. При этом может обеспечиваться несанкционированный доступ к персональным данным или реализовываться угроза отказа в обслуживании. Особенно опасны угрозы, когда ИСПДн представляет собой распределенную информационную систему, подключенную к сетям общего пользования или сетям международного информационного обмена.

Среди всех угроз данного типа, можно выделить семь наиболее часто реализуемых в настоящее время.

1. Анализ сетевого трафика Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель изучает логику работы сети — то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней, перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по

протоколам FTP и TELNET, не предусматривающим шифрование), ее подмены, модификации и т.п. На рисунке приложения 5 представлена схема реализации такой угрозы.

2. Сканирование сети. Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель — выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

3. Угроза выявления пароля. Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник реализовывает угрозу с помощью ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

4. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения. Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения имеет место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных. В результате реализации угрозы нарушитель получает права доступа, установленные его пользователем для доверенного абонента, к техническому средству ИСПДн – цели угроз. Схема реализации данной угрозы представлена на схеме в приложении 6.

5. Навязывание ложного маршрута сети. Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими

алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

6. Внедрение ложного объекта сети. Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае, если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

7. Отказ в обслуживании. Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты. Можно выделить несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-

эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

- явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;
- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, какое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полную остановку компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

8. Удаленный запуск приложений. Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых — нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Схематично основные этапы работы этих программ выглядят так:

- инсталляция в памяти;
- ожидание запроса с удаленного хоста, на котором запущена клиент-программа, и обмен с ней сообщениями о готовности;
- передача перехваченной информации клиенту или предоставление ему контроля над атакуемым компьютером.

Возможные последствия реализации угроз различных классов перечислены далее, в таблице приложения 7.

2.3.4. Угрозы программно-математических воздействий

Программно-математическое воздействие — это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, уничтожение, блокирование и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены как преднамеренно, так и случайно в программное обеспечение, используемое в ИСПДн, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИСПДн с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИСПДн.

Наличие в ИСПДн вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную и криптографическую защиту.

Основными видами вредоносных программ являются:

- программные закладки;
- классические программные (компьютерные) вирусы;
- вредоносные программы, распространяющиеся по сети (сетевые черви);

- другие вредоносные программы, предназначенные для осуществления НСД.

Классификация программных вирусов и сетевых червей представлена на схеме в приложении 8.

2.4. Угрозы безопасности персональных данных, обрабатываемых в автоматизированных рабочих местах, имеющих подключение к сетям связи общего пользования или сетям международного информационного обмена

При обработке персональных данных на автоматизированном рабочем месте, имеющем подключения к сетям связи общего пользования или сетям международного информационного обмена, возможна реализация следующих угроз безопасности персональных данных:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.
- угрозы утечки информации по техническим каналам включают в себя:
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теми же условиями и факторами, что и для автоматизированного рабочего места (АРМ), не имеющего подключения к сетям общего пользования или сетям международного информационного обмена.

Угрозы НСД в ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена.

Угрозы НСД в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования. Угрозы из внешних сетей включают в себя:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;

- угрозы получения НСД путем подмены доверенного объекта; угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

Все потенциальные угрозы, перечисленные в данном разделе, было описаны в предыдущих разделах (2.1–2.3.4).

Глава 3. Модель защиты

Согласно методическому документу «Меры защиты информации в государственных информационных системах» утвержденному ФСТЭК России 11 февраля 2014 года, организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от ранее перечисленных угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостность информационной системы информации;
- обеспечение доступности информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств и систем связи и передачи данных.

3.1. Идентификация и аутентификация субъектов и объектов доступа

При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора, и процессов,

запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной аутентификации — определенной комбинации указанных средств.

В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

Для защиты персональных данных в ИСПДн должны осуществляться следующие меры защиты:

- идентификация и аутентификация устройств
- управление идентификаторами пользователей и устройств;
- управление средствами аутентификации;
- идентификация и аутентификация внешних пользователей.

3.2. Управление доступом субъектов доступа к объектам доступа

Для безопасного функционирования информационной системы персональных данных оператором должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей;
- реализация необходимых методов управления доступом (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);

- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- регламентация и контроль использования в информационной системе технологий беспроводного доступа;
- регламентация и контроль использования в информационной системе мобильных технических средств;
- управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

3.3. Ограничение программной среды

Согласно методике ФСТЭК, указанной в ссылке [5], автоматизированной информационной системе, обрабатывающей и хранящей персональные данные, располагающейся на коммерческом предприятии, должны выполняться следующие требования по ограничениям программной среды (ОПС):

- управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения;
- управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения;
- установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.

3.4. Защита машинных носителей информации

В автоматизированной информационной системе предприятия должны быть реализованы требования к защите машинных носителей:

- оператором должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации;
- оператором должны быть реализованы функции по управлению доступом к машинным носителям информации, используемым в информационной системе;

- оператором должен обеспечиваться контроль перемещения используемых в информационной системе машинных носителей информации за пределы контролируемой зоны;
- оператором должно обеспечиваться исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, или использования носителей информации в иных информационных системах;
- в информационной системе должен осуществляться контроль использования интерфейсов ввода (вывода);
- должен осуществляться контроль ввода (вывода) информации на машинные носители информации;
- должен обеспечиваться контроль подключения машинных носителей информации.
- оператором должно обеспечиваться уничтожение информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль стирания информации.

3.5. Регистрация событий безопасности

К событиям безопасности, подлежащим регистрации в информационной системе, относят любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации в системе обработки персональных данных. Для АИС обязательное соблюдение требований регистрации событий безопасности (РСБ):

- оператором должны быть определены события безопасности в информационной системе, подлежащие регистрации, и сроки их хранения;
- в информационной системе должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации;
- в информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности;
- в информационной системе должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки,

сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;

- в информационной системе должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени;
- в информационной системе должна обеспечиваться защита информации о событиях безопасности;
- в информационной системе должна иметься возможность просмотра и анализа информации о действиях отдельных пользователей в информационной системе.

3.6. Антивирусная защита

Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации. Кроме того, оператором должно быть обеспечено регулярное обновление базы данных признаков вредоносных компьютерных программ (вирусов).

3.7. Обнаружение вторжений

Оператором должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений. Также оператором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе.

3.8. Контроль (анализ) защищенности информации

В АИС в рамках анализа защищенной информации (АЗИ) оператором должны выполняться следующие действия:

- поиск, анализ и устранение уязвимостей в информационной системе;

- контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода;
- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.;
- контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация);
- контроль правил генерации паролей пользователей, ведения учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

3.9. Обеспечение целостности информационной системы и информации

В информационной системе должен осуществляться контроль целостности следующих компонентов системы:

- контроль программного обеспечения, в т.ч. ПО средств защиты информации;
- контроль целостности информации, содержащейся в базах данных информационной системы;
- контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и т.д.), и исключение неправомерной передачи информации из ИС;
- контроль точности, полноты и правильности данных, вводимых в информационную систему;
- контроль ошибочных действий пользователей по вводу или передаче информации и предупреждение пользователей об ошибочных действиях.

Оператором в текущем аспекте должно быть выполнено следующее:

- предусмотрена возможность восстановления программного обеспечения, включая ПО средств защиты информации, в нештатных ситуациях;
- должно обеспечиваться реагирование на поступление незапрашиваемых электронных сообщений, не относящихся к функционированию ИС (защита от спама).
- должно осуществляться ограничение прав пользователей по вводу информации в информационную систему.

3.10. Обеспечение доступности информации

В разделе обеспечения доступности информации в АИС на оператора возлагаются следующие обязанности:

- должно обеспечиваться использование отказоустойчивых технических средств;
- должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы;
- должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;
- должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации;
- должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала;
- должно обеспечиваться выделение групп однотипных узлов, объединенных каналами передачи информации и рассматриваемых как единый программно-технический ресурс, информационной системы в целом или отдельных сегментов (серверов приложений, баз данных, файловых серверов, СЗИ и иных сегментов) для обеспечения доступности информации, механизмов защиты информации; должен осуществляться контроль состояния и качества предоставления провайдером вычислительных ресурсов в т. ч. по передаче информации.

3.11. Защита технических средств

Оператором должна обеспечиваться защита информации, обрабатываемой техническими средствами, от ее утечки за счет побочных электромагнитных излучений и наводок. Также к оператору должен:

- обеспечивать контролируемую зону, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования;
- обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены,

исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены;

- осуществлять размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;
- осуществлять защиту от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

Заключение

В процессе изучения темы был разработан алгоритм защиты персональных данных в автоматизированной системе коммерческого предприятия на основании описания основные принципы классификации автоматизированных систем коммерческих предприятий, модели угроз и методов защиты, присущих классу автоматизированной системы 1В.

Проведён анализ современных подходов к классификации информационных систем, который показывает, что не существует единой методики классификации всех автоматизированных систем, в современных законах есть общие принципы разделения на классы и группы.

Спланированная модель угроз показала, что в современных реалиях существует большое количество потенциальных угроз для автоматизированных систем, содержащих персональные данные, относящихся к типу 1В. Раздел «модель защиты» доказывает, что перечисленные ранее потенциальные угрозы возможно предотвратить если использовать принципы и устройства защиты, описанные в данном разделе.

Экономическая эффективность применения предложенных технических решений обоснована масштабом организации и ценностью информации, содержащейся в ее автоматизированной системе.

Библиографический список

1. Федеральный закон Российской Федерации №152 «О персональных данных» от 27 июля 2006 г. [Электронный ресурс] сайт. – URL: <https://rg.ru/2006/07/29/personalnnye-dannye-dok.html>
2. Постановление Правительства Российской Федерации №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. [Электронный ресурс] сайт. – URL: <https://rg.ru/2012/11/07/pers-dannye-dok.html>

3. Приказ №21 ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. [Электронный ресурс] сайт. – URL: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21>

4. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] сайт. – URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsdatelya-gostekhkommisii-rossii-ot-30-marta-1992-g>

5. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г. [Электронный ресурс] сайт. – URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument>

6. Приказ №17 ФСТЭК «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г. [Электронный ресурс] сайт. – URL: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17>

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России от 15 февраля 2008 г. [Электронный ресурс] сайт. – URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god>

Приложение 1

Требования к классам защищенности и к автоматизированной системе

Подсистемы и требования	Классы			АС
	1В	1Г	1Д	
1. Подсистема управления доступом				
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:				
в систему	+	+	+	+
к терминалам, электронно-вычислительным машинам (ЭВМ), узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	+	+	-	+
к программам	+	+	-	+
к томам, каталогам, файлам, записям, полям записей	+	+	-	+
1.2. Управление потоками информации	+	-	-	+
2. Подсистема регистрации и учета				
2.1. Регистрация и учет:				
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+
выдачи печатных (графических) выходных документов	+	+	-	+
запуска (завершения) программ и процессов (заданий, задач)	+	+	-	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	+	+	-	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	+	+	-	+
изменения полномочий субъектов доступа	+	-	-	+
создаваемых защищаемых объектов доступа	+	-	-	+
2.2. Учет носителей информации	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+	+	-	+
2.4. Сигнализация попыток нарушения защиты	+	-	-	+
3. Криптографическая подсистема	+	+	+	+
4. Подсистема обеспечения целостности				
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	+	-	-	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+
4.6. Использование сертифицированных средств защиты	+	-	-	+

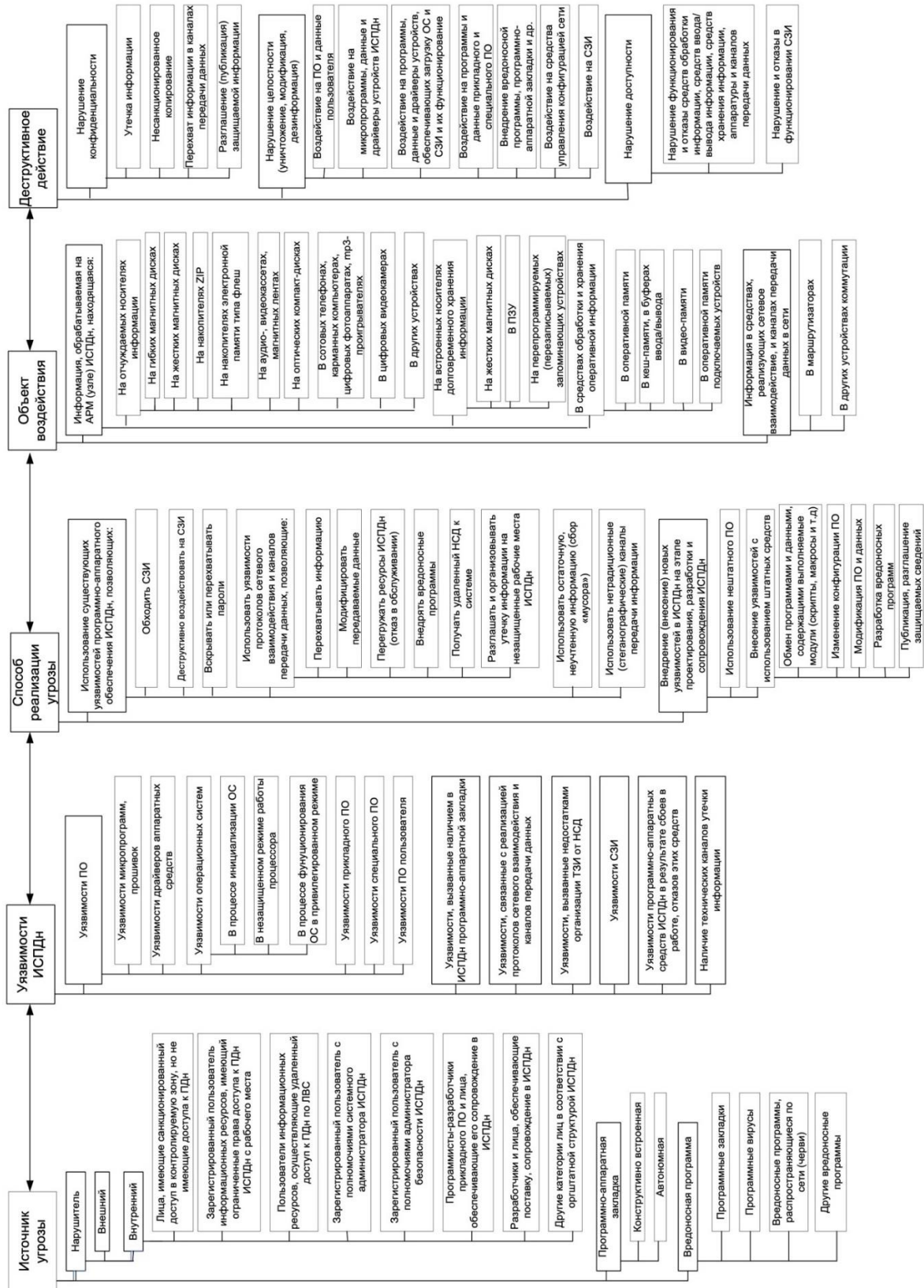
Обозначения:

" - " - нет требований к данному классу;

" + " - есть требования к данному классу.

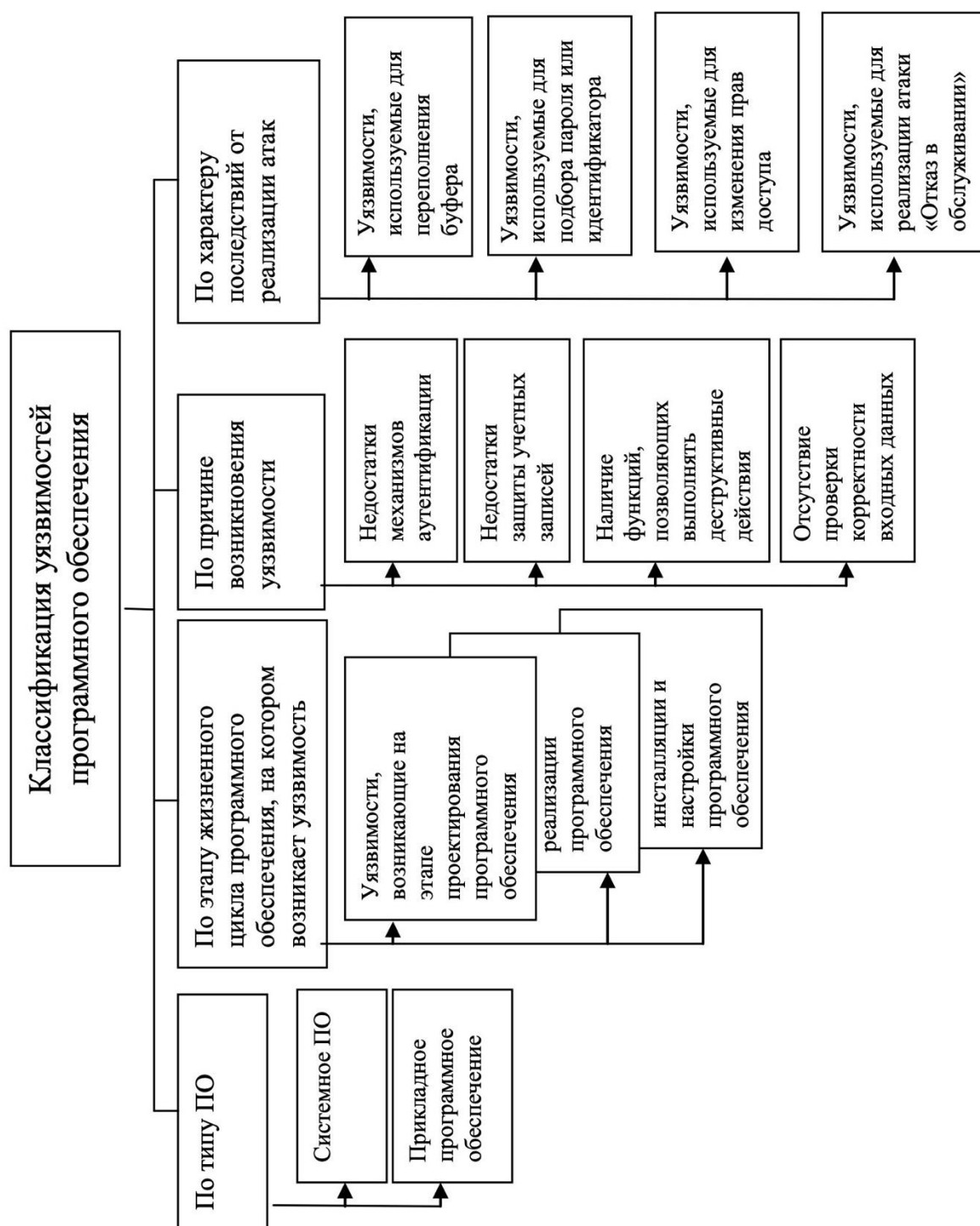
Приложение 2

Элементы описания угроз НСД к информации в ИСПДн



Приложение 3

Классификация уязвимостей программного обеспечения



Приложение 4

Уязвимости отдельных протоколов стека протоколов TCP/IP, на базе которого функционируют глобальные сети общего пользования

Наименование протокола	Уровень стека протоколов	Наименование (характеристика) уязвимости	Содержание нарушения безопасности информации
FTP (File Transfer Protocol) – протокол передачи файлов по сети	Прикладной, представительный, сеансовый	1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) 2. Доступ по умолчанию 3. Наличие двух открытых портов	Возможность перехвата данных учетной записи (имен зарегистрированных пользователей, паролей). Получение удаленного доступа к хостам
telnet – протокол управления удаленным терминалом	Прикладной, представительный, сеансовый	Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)	Возможность перехвата данных учетной записи пользователя. Получение удаленного доступа к хостам
UDP – протокол передачи данных без установления соединения	Транспортный	Отсутствие механизма предотвращения перегрузок буфера	Возможность реализации UDP-шторма. В результате обмена пакетами происходит существенное снижение производительности сервера
ARP – протокол преобразования IP-адреса в физический адрес	Сетевой	Аутентификация на базе открытого текста (информация пересылается в незашифрованном виде)	Возможность перехвата трафика пользователя злоумышленником
RIP – протокол маршрутной информации	Транспортный	Отсутствие аутентификации управляющих сообщений об изменении маршрута	Возможность перенаправления трафика через хост злоумышленника
TCP – протокол управления передачей	Транспортный	Отсутствие механизма проверки корректности заполнения служебных заголовков пакета	Существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP
Наименование протокола	Уровень стека протоколов	Наименование (характеристика) уязвимости	Содержание нарушения безопасности информации
DNS – протокол установления соответствия мнемонических имен и сетевых адресов	Прикладной, представительный, сеансовый	Отсутствие средств проверки аутентификации полученных данных от источника	Фальсификация ответа DNS-сервера
IGMP – протокол передачи сообщений о маршрутизации	Сетевой	Отсутствие аутентификации сообщений об изменении параметров маршрута	Зависание систем Win 9x/NT/200
SMTP – протокол обеспечения сервиса доставки сообщений по электронной почте	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность подделывания сообщений электронной почты, а также адреса отправителя сообщения
SNMP – протокол управления маршрутизаторами в сетях	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность переполнения пропускной способности сети

Приложение 5

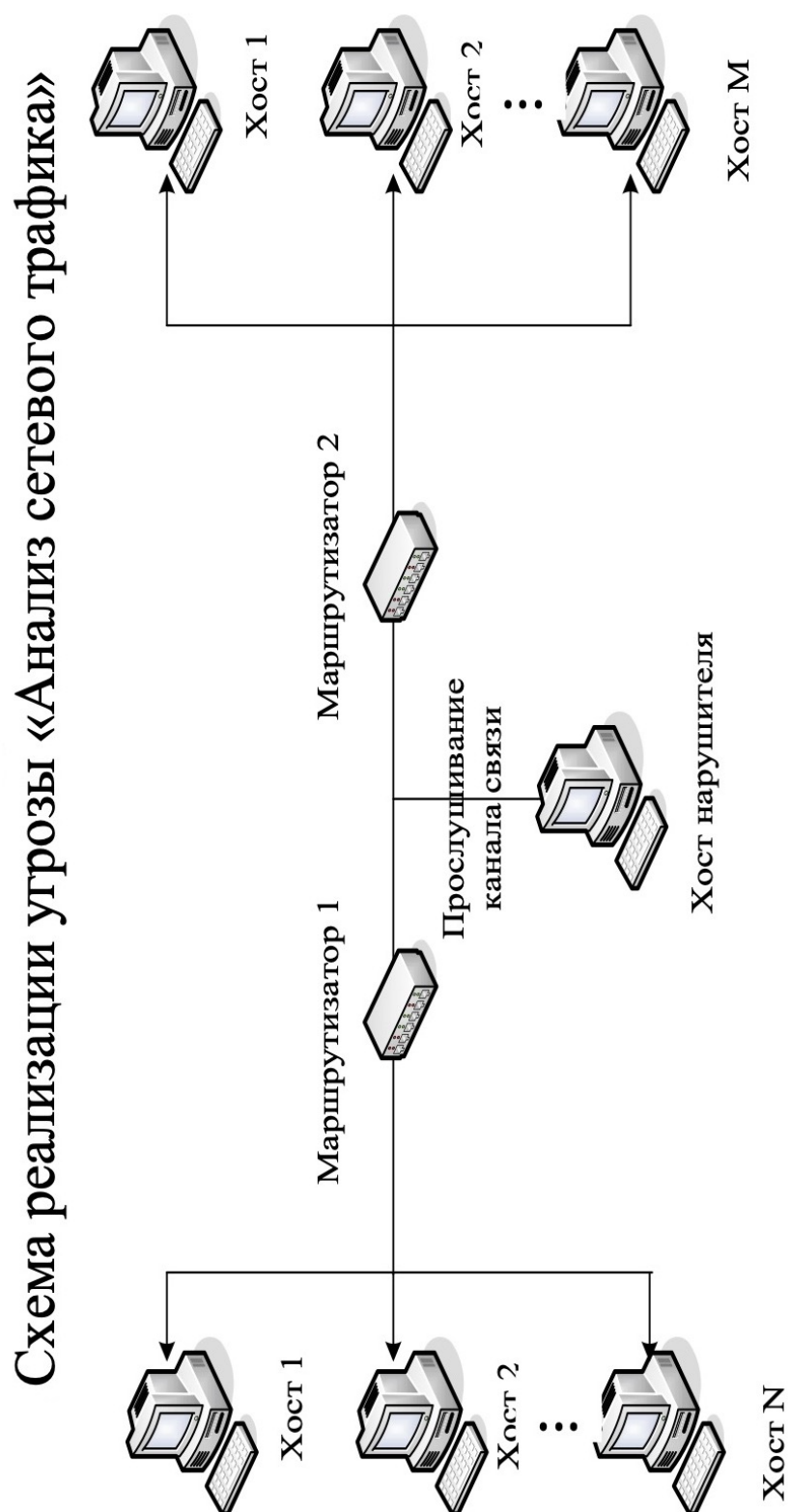


Схема реализации угрозы «Подмена доверенного объекта сети»

Хост X - хост нарушителя

Хост А - доверенный хост

Хост В

Diagram illustrating the first step of a TCP connection:

- Host X (Хост X) sends a SYN packet and its initial sequence number (ISS_x) to Host A (Хост А).
- Host A is labeled "время хост А" (time of host A).
- Host B (Хост В) is shown on the right, but no connection is established yet.

Хост X

SYN,
ISSx

Хост B

TCP-запрос на открытие соединения от имени хоста А
 SYN-бит синхронизации номера последовательности
 ISSx-произвольный номер последовательности
 хост А выведен из строя

Хост X

Хост А

Хост В

Ответ хоста В на TCP-запрос

SYN, ACK, ISSb
ACK(ISSx+1)

SYN-бит синхронизации номера последовательности
ISSb-произвольный номер последовательности хоста В
ACK(ISSx+1)-номер подтверждения приема TCP-пакета от
хоста А, равный ISSx+1

Хост X

Хост B

ASK(ISSb+1)-номер подтверждения приема TCP-пакета от хоста B, в котором атакующий указывает подобранный номер ISSb+1

ACK, ISSx+1

ACK(ISSb+1)

ASK(ISSx+1)-номер следующего TCP-пакета

Отсутствует сообщение о разрыве TCP-соединения от выведенного из строя хоста A (пакет с заполненным служебным заголовком RST)

Приложение 7

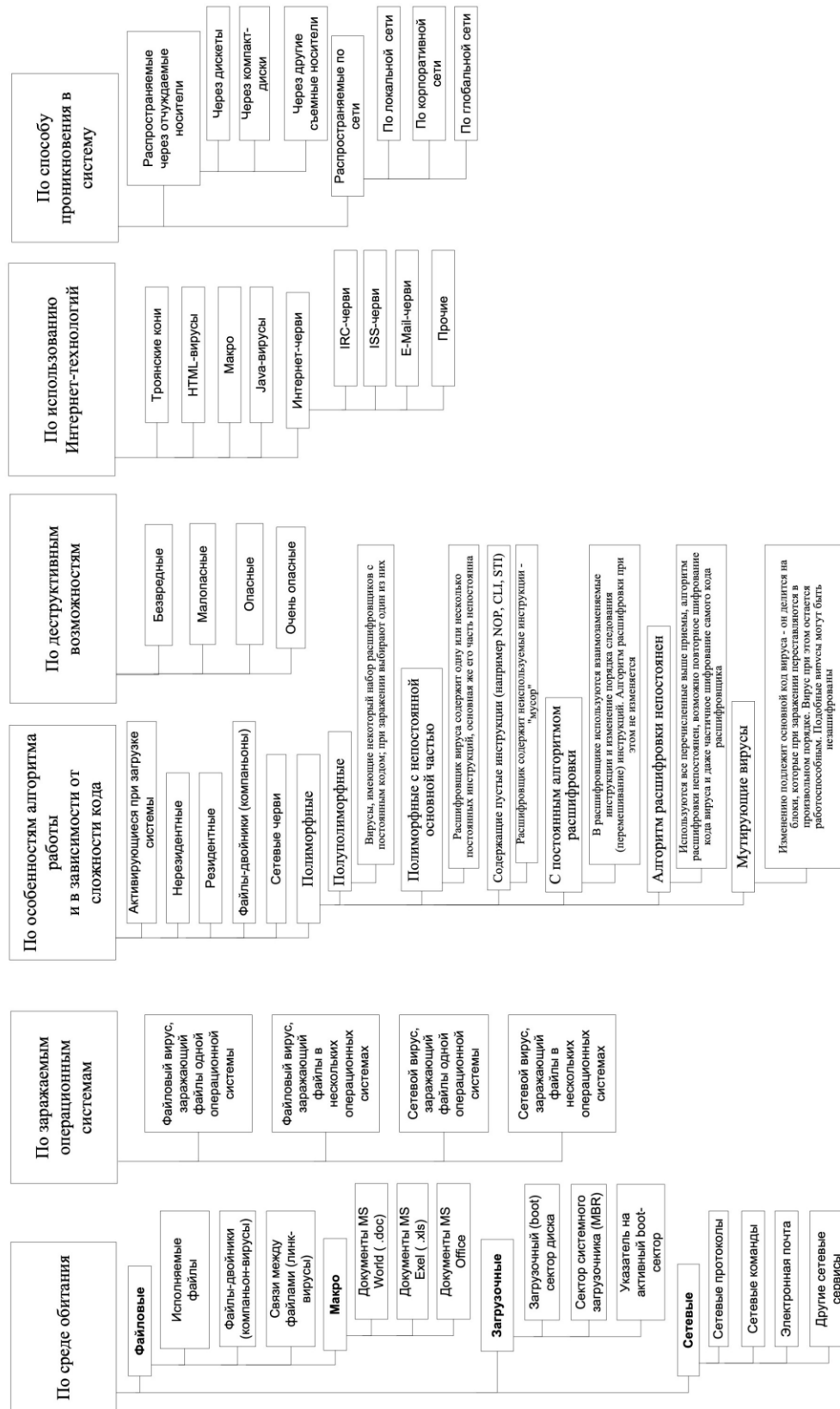
Возможные последствия реализации угроз различных классов

№ п/п	Тип атаки		Возможные последствия
1	Анализ сетевого трафика		Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
2	Сканирование сети		Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
3	«Парольная» атака		Выполнение любого деструктивного действия, связанного с получением несанкционированного доступа
4	Подмена доверенного объекта сети		Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно- адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
5	Навязывание ложного маршрута		Несанкционированное изменение маршрутно- адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
6	Внедрение ложного объекта сети		Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
7	Отказ в обслуживании	Частичное истощение ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение
		Полное истощение ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.д.)
		Нарушение логической связности между атрибутами, данными, объектами	Невозможность передачи, сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
		Использование ошибок в программах	Нарушение работоспособности сетевых устройств

№ п/п	Тип атаки		Возможные последствия
8	Удаленный запуск приложений	Путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации
		Путем переполнения буфера серверного приложения	
		Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой

Приложение 8

Классификация программных вирусов и сетевых червей



Финансы, денежное обращение и кредит

УДК 33

Панова А.Ю., Мамедова А.Р. Потребительское кредитование в России в период пандемии Consumer lending in Russia during a pandemic

Панова Анастасия Юрьевна

Российский государственный гидрометеорологический университет, доцент кафедры экономики предприятия природопользования и учетных систем

Мамедова Асли Рауфовна

Российский государственный гидрометеорологический университет, Бакалавр

Panova Anastasia Yurievna

Russian State Hydrometeorological University, Associate Professor of the Department of Economics of Environmental Management Enterprise and Accounting Systems

Mamedova Asli Raufovna

Russian State Hydrometeorological University, Bachelor

Аннотация. Статья посвящена изменению потребительского кредитования в России во время пандемии COVID-19. В статье проведен анализ статистических данных о динамике потребительского кредитования, влиянии изменений ключевой ставки на ставки по кредитам, выданным населению. Внимание уделено результатам ужесточившихся процедур андеррайтинга, вопросам формирования просроченной задолженности и реструктуризации кредитов в РФ в период пандемии.

Ключевые слова: потребительское кредитование, пандемия COVID-19, ключевая ставка

Abstract. The article is devoted to the change in consumer lending in Russia during the COVID-19 pandemic. The article analyzes statistical data on the dynamics of consumer lending, the impact of changes in the key rate on interest rates on loans issued to the population. Attention is paid to the results of toughened underwriting procedures, the formation of overdue debts and the restructuring of loans in the Russian Federation during a pandemic.

Keywords: consumer lending, COVID-19 pandemic, key rate

DOI 10.54092/25420208_2021_9_52

Рецензент: Бессарабов Владислав Олегович - Кандидат экономических наук. ГО ВПО «ДонНУЭТ имени Михаила Туган-Барановского»

Введение.

Потребительское кредитование является самым распространенным видом банковских операций во многих странах, потому что при помощи данного вида займа увеличивается ёмкость рынка по целому ассортименту потребительских товаров и недвижимого имущества и с позиции кредитора они приносят значительную прибыль. Однако пандемия COVID-19 вносит свои коррективы в условия потребительских займов, что влияет на многие сферы экономики, а также влечет за собой изменение поведения физических лиц, при сокращении заработной платы или потери рабочего места.

Объект и методы исследования.

Различные формы и виды потребительского кредитования повышают уровень жизни населения страны, ускоряют товарооборот и создают «климат» для развития и ускорения производства, тем самым в обществе снижается социальная напряженность в результате дополнительных возможностей для широких слоев населения. Банк России в ходе проведения денежно-кредитной политики имеет возможность регулировать процессы кредитования, проводя политику дорогих или дешевых денег. Потребительское кредитование в период пандемии COVID-19 является предметом данной статьи. В качестве методов исследования использованы сравнительный анализ и описание.

Экспериментальная часть. В 2018-2019 годах стремительно начал расти такой сегмент кредитного рынка, как потребительское кредитование. Это объясняется тем, что еще с 2016 г. постепенно начали снижаться ставки по потребительскому кредитованию. Связано такое явление было с тем, что Банк России активно проводил денежно-кредитную политику дешевых денег. Рассмотрим динамику потребительского кредитования (Рис. 1) в период с 2019 – 2021гг. Потребительское кредитование имеет выраженную сезонность, традиционно снижение происходит в первом квартале, а в четвертом – рост, поэтому на рисунке 3 значения приведены поквартально. При сравнении данных за первый квартал, видим неуклонный рост, но во втором квартале 2020 г. можно наблюдать резкий спад объема потребительского кредитования. Падение объема портфеля в первом полугодии 2020 года, в особенности с апреля по июнь, а так же объем выданных кредитов населению на личные нужды в среднем на 40% ниже уровня предыдущего квартала. Основной причиной такого явления стала пандемия коронавируса, а затем и объявление локдауна в середине марта. Потенциальные заемщики рассматривают ситуацию в целом как высокорисковую и собственное финансовое положение считают нестабильным, в результате чего спрос на кредитование снижается. Коммерческие банки также отмечают рост рисков в сфере кредитования населения и, в результате снижают объем выдаваемых ссуд.

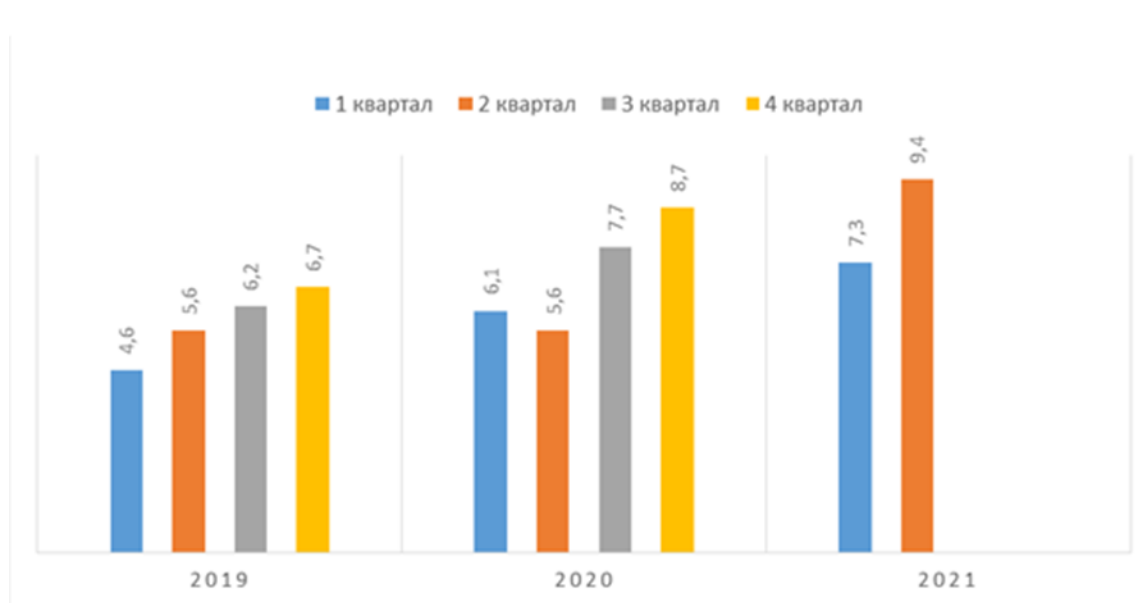


Рисунок 1. Потребительские кредиты, предоставленные физическим лицам за период с 2019 по 2021 год, млн. руб. [составлено авторами на основании данных Банка России]

Рассмотрим воздействие регулятора на рынок потребительского кредитования за период 2018-2021 гг., рис. 2. Центральный Банк с помощью денежно-кредитной политики пытается поддержать стабильность в экономике России, тем самым повышая или понижая ключевую ставку. Мы видим динамику ключевой ставки ЦБ РФ поквартально за период 2018-2021 гг.

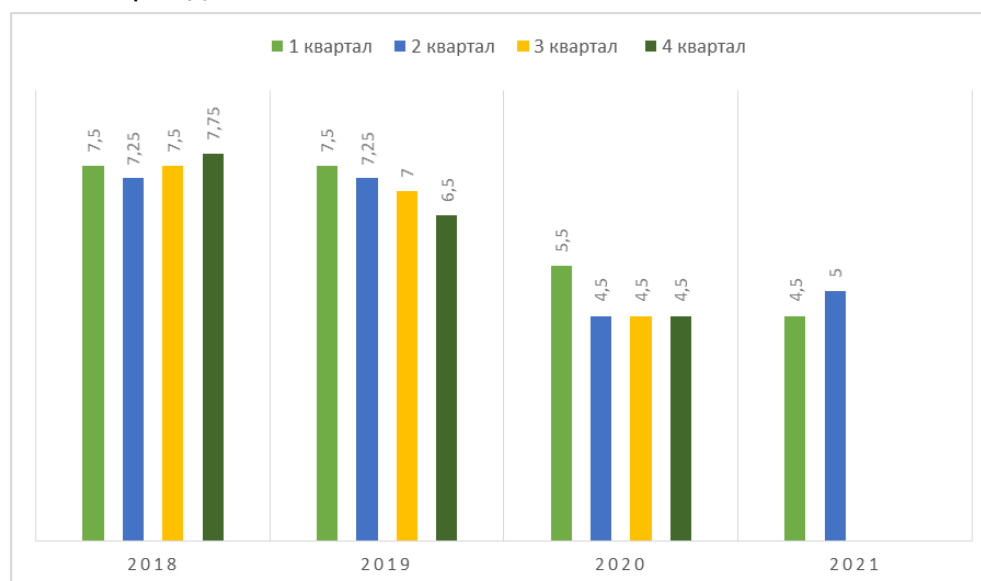


Рисунок 2. Динамика ключевой ставки ЦБ РФ за период с 2018 по 2021 год [2]

Сумма долга по потребительским ссудам за тот же период увеличилась в 1,5 раза. Увеличение кредитной задолженности населения и особенно бурный рост просроченной задолженности по долгам населения тревожил Центральный банк России. Однако в 2020-2021 гг. на фоне резкого снижения потребительского кредитования, ввиду первой и второй волны коронавирусной пандемии, Совет директоров ЦБ РФ 19 июня 2020 г. принял решение снизить ключевую ставку до 4,5% годовых, что ниже соответствующего показателя годичной давности более, чем на треть. Принятые ЦБ решения по ключевой ставке создали условия для снижения процентных ставок на всех сегментах финансового рынка. Так, на рисунке 3 мы можем видеть средние ставки по потребительским кредитам без учета влияния Сбербанка. Сбербанк – это банк с государственным участием и изменение им ставок по потребительским кредитам может носить административный характер, в то же время коммерческие банки используют рыночную модель принятия решения по ставкам потребительского кредитования.

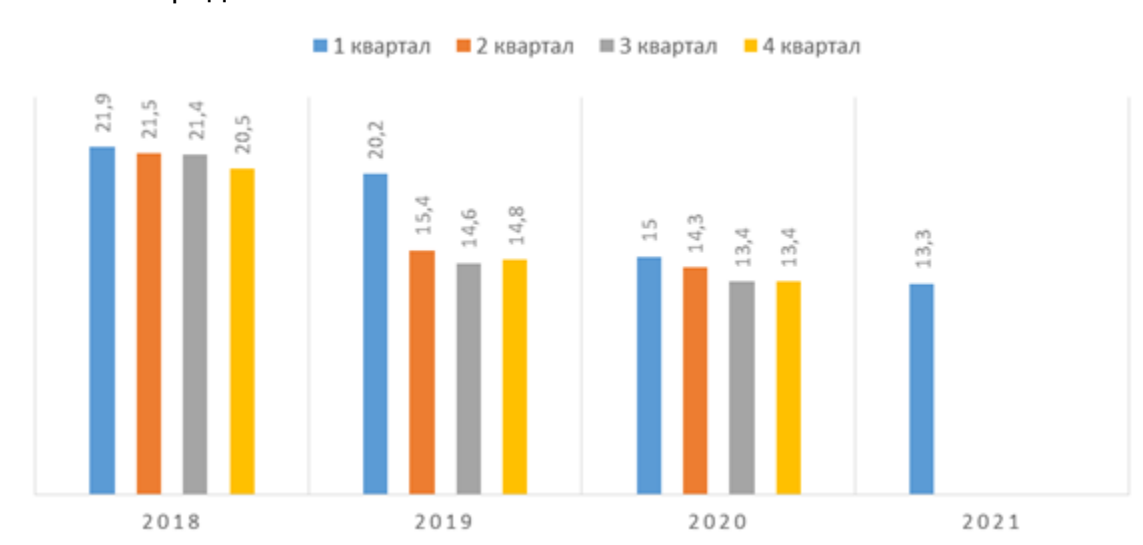


Рисунок 3. Средние ставки по потребительским кредитам за период с 2018 по 2021 год, % [3]

Во втором квартале 2020 г. снизились под влиянием снижения ключевой ставки средние ставки по потребительским кредитам во время коронавирусной пандемии и составили 14,3% годовых; падение ставок продолжалось и в третьем-четвертом квартале, и они достигли 13,4% годовых, что повлекло за собой увеличение портфеля потребительских кредитов в 3 и 4 квартале 2020 г. – до 8,7 млн.руб.

Результаты. Начиная с апреля 2020 года, банки начали повышать требования к истории кредитных обязательств и ПДН (показателю кредитной нагрузки) для комфортного обслуживания задолженности потенциальных клиентов без вреда для

финансового положения. Таким отраслям предпринимательства, как ресторанный бизнес, розничная торговля, бытовые услуги и гостиничный бизнес банки стали уделять повышенное внимание ввиду неустойчивости доходов населения. Коммерческие банки пытались максимально минимизировать риски, снизив размеры выдаваемых ссуд физическим лицам. Особенно это снижение наблюдалось по наличным займам, поскольку, как правило, сумма такого займа больше, чем в других сегментах кредитования физических лиц. Новых клиентов коммерческие банки пытались найти среди обслуживаемых зарплатных проектов, то есть когда банки автоматически перечисляют заработную плату, премии, командировочные на карту сотрудников определенного предприятия. В результате ужесточившихся процедур андеррайтинга существенно сократилась степень одобрения кредитных заявлений. Так, на рис. 4 мы наблюдаем увеличение доли кредитов за январь-июнь 2020 года наличными в портфеле потребительских ссуд – с 72,6 до 73,2%. Таким образом, в 2020 году было выдано 14,57 млн.ед. кредитов на покупку потребительских товаров, это на 25,9% меньше, чем в 2019 году (19,68 млн.ед.) [4].

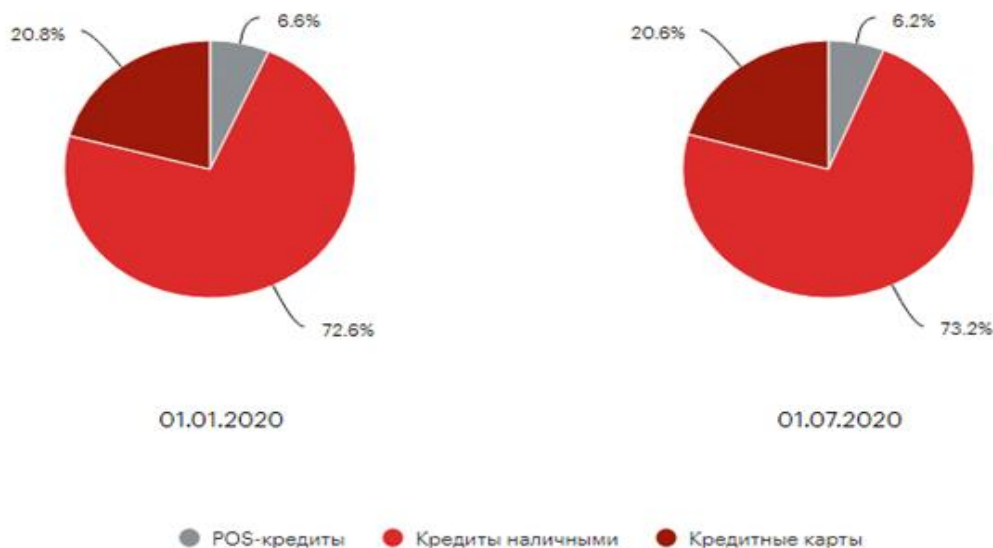


Рисунок 4. Результат ужесточившихся процедур андеррайтинга в 2020 году [4]

3 апреля 2020 года Государственной Думой был принят закон «О внесении изменений в Федеральный закон «О Центральном Банке РФ» и отдельные законодательные акты Российской Федерации в части особенностей изменения условий кредитного договора, договора займа» [5]. Данный закон обеспечил кредитные каникулы до 6 месяцев населению, удовлетворяющему определенным условиям. Стараясь поддержать население во время пандемии COVID-19 принятый закон позволил предоставить кредитные отпуска до полугода, а также уменьшить

неблагоприятные воздействия на финансовые показатели банков. В условиях сокращения, а порой и потери доходов населения, Центральный Банк рекомендовал коммерческим банкам предлагать клиентам новые программы реструктуризации задолженности. Банки должны были рассмотреть заявки заемщиков о просьбе реструктуризации долга, например, не начислять штрафы и пени, то есть максимально удовлетворить своих клиентов вовремя локдауна. Кредитные каникулы привели к значительному падению доходов в банковском секторе. Всего с января по июнь были реструктурированы долги физических лиц в объеме 625 млн.руб., примерно 313 млн.руб. приходится на частные кредиты (около 4% от общей задолженности населения), тем не менее значительная часть реструктуризаций по новой программе приходится по кредитам наличными. После прохождения первой волны коронавирусной инфекции доля реструктуризаций кредитов достигает 3,6%, рост продолжается и в первом полугодии 2021 года (4,1%). Доля просроченной задолженности по кредитам ФЛ в 2020 году вырос до 20%. Просроченные обязательства по всем кредитам выросли более чем на 100 млрд.руб., в основном в сегменте кредитов наличными (560 млрд.руб.) и кредитных карт (153 млрд.руб.). Просроченная задолженность физических лиц на январь-июнь 2020 года увеличились на 4%, а на июль-октябрь составила всего 4,7% от кредитного портфеля, увеличение происходит и в 2021 году достигая 20,1%, что мы и наблюдаем на рис.5.

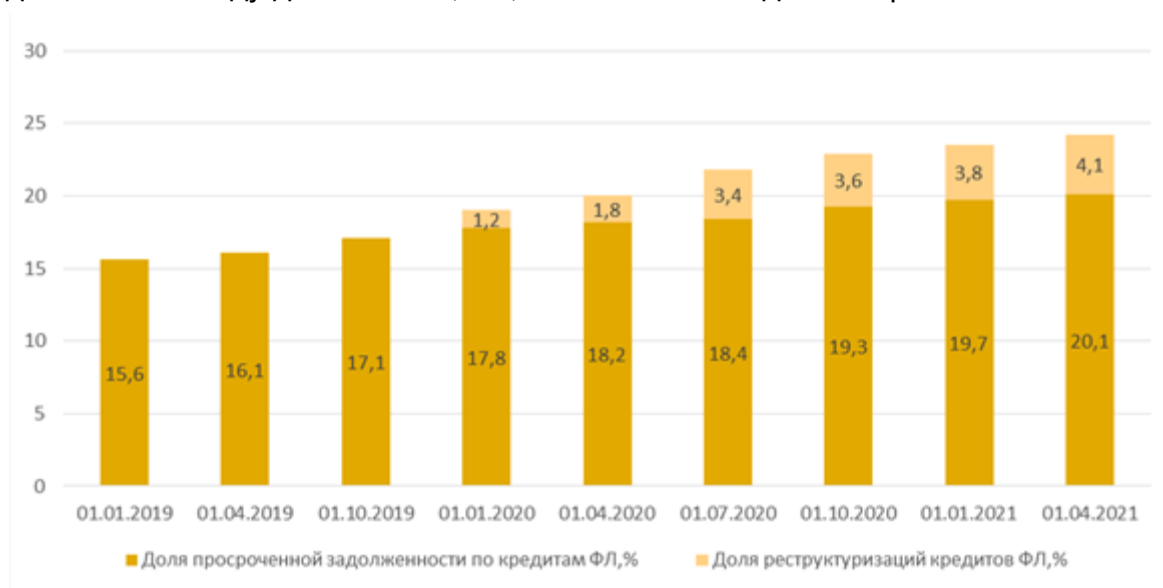


Рисунок 5. Просроченная задолженность и реструктуризация кредитов, выданных физическим лицам, за период с 2019 по 2021 год [6]

Заключение. Пандемия коронавируса оказала влияние на банковский сектор, однако сравнивая кризисы 2008-2009 гг. и 2014-2015 гг. с современной ситуацией, можно сказать, что российский банковский сектор является более стабильным. Изменения произошли из-за макроэкономических факторов, снижения доходов населения и ухудшения кредитной истории не только у юридических лиц, но и физических. Почти во всем мире был введен карантинный режим, ограничения для многих видов деятельности и были закрыты большинство международных границ. Подобные мероприятия были необходимы, и это вызвало серьезные экономические последствия для всего мира. Центральный банк и государство вводили меры поддержки не только для населения, но и для экономики в целом, с целью стабилизации положения на финансовых рынках. Банк России решил смягчить монетарную политику, тем самым за год, снизив ставки до 4,5% годовых, и обеспечил стабильность и непрерывность работы финансовых учреждений. Это позволило населению приобретать более дешевые кредиты и тем самым создало предпосылки для этапа восстановления экономики. Государство стремительно принимало законы с целью разработки и проведению антикризисных мер, а также для поддержки населения разработало программу льготного кредитования под 6,5%. Впоследствии коммерческими банками были приняты меры по ужесточению одобрений кредитов, в том числе и предоставлению ссуд населению для удовлетворения своих нужд.

Рассмотрев ситуацию на рынке потребительского кредитования можно сделать вывод о том, что сложившаяся ситуация в 2020 г. повлияла на население и банковский сектор. В случае введения новых ограничений в разных сферах экономики на фоне новой волны коронавирусной инфекции или макроэкономических проблем (в виде дополнительных санкций и/или падения цены на нефть) могут в первую очередь повлиять на рынок потребительского кредитования. Во время карантина россияне перешли к сберегательной модели поведения, пересмотрев свои покупательские привычки. Это может повлечь за собой снижение платежеспособного спроса потребителя, что может негативно сказаться на состоянии малого и среднего бизнеса и, возможно, потерю рабочих мест. Коммерческим банкам в период карантинных мер приходится изменить и технологическую возможность, наращивая дистанционное обслуживание.

23 июля 2021 года Центральным Банком России было решено поднять ключевые ставки до 6,5% годовых, а 10 сентября 2021 года Совет директоров Банка России повысил ключевую ставку на 25 б.п., до 6,75% годовых. Такое решение было принято в силу того, что во втором квартале 2021 года экономическая ситуация достигла допандемического уровня. Динамика индекса потребительских цен является основным фактором, влияющим на динамику ключевой ставки. По итогам 2020 года индекс

потребительских цен составил 4,9%, вместо прогнозируемых 4%. Также нельзя забывать про рост инфляции, который достиг 6% годовых. Высокий уровень инфляционных ожиданий, мотивируют Банк России изменить приоритеты в пользу проинфляционных, что может привести к дальнейшему росту инфляции. Таким образом, Центральный банк решил перейти к нейтральной процентной ставке, сохраняя баланс между давлением на среднее изменение цен на товары и услуги и прессингом на уровень деловой активности [7].

Библиографический список

1. Банк России, Сведения о кредитах, предоставленных физическим лицам. [Электронный ресурс]. – <https://cbr.ru/statistics/pdko/f316/f316-info/?fdate=202101®n=1481>
2. Банк России, Ключевая ставка Банка России. [Электронный ресурс]. – Режим доступа: https://cbr.ru/hd_base/keyrate/?UniDbQuery.Posted=True&UniDbQuery.From=01.01.2021&UniDbQuery.To=30.04.2021
3. Банк России, Средневзвешенные процентные ставки по кредитным и депозитным операциям в рублях без учета ПАО Сбербанк. [Электронный ресурс]. – Режим доступа: https://cbr.ru/statistics/bank_sector/int_rat/
4. РА Эксперт, Обзор рынка потребительского кредитования по итогам 1-го полугодия 2020 года. [Электронный ресурс]. – Режим доступа: https://raexpert.ru/researches/banks/potrebcred_1h2020
5. Верховный Суд РФ, Федеральный закон от 03.04.2020 № 106-ФЗ о кредитных каникулах. [Электронный ресурс]. – Режим доступа: <https://www.vsr.ru/documents/all/28882/#:~:text=Ответ%3A%20Федеральным%20законом%20от%203,требованию%20заемщика%20-%20физического%20лица%2C>
6. Банк России, Динамика реструктуризации кредитов населения и бизнеса. [Электронный ресурс]. – Режим доступа: <https://cbr.ru/analytics/drknb/>
7. Банк России, Новости. [Электронный ресурс]. – Режим доступа: https://cbr.ru/press/pr/?file=23072021_133000Key.htm

Экономика предпринимательства

УДК 338.462

Балашова Р.И., Гречина И.В., Леонова Л.А. Эффективность сферы услуг региональной экономики: субъекты предпринимательства, инновации, территория

Efficiency of the service sector of the regional economy: business entities, innovations, territory

Балашова Раиса Ивановна

Институт экономических исследований, г. Донецк

Гречина Ирина Викторовна

Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского, г. Донецк,

Леонова Лилия Александровна

Донецкий национальный технический университет, г. Донецк

Balashova Raisa Ivanovna

Economic Research Institute, Donetsk

Grechina Irina Viktorovna

Donetsk National University of Economics and Trade named after Mikhail Tugan-Baranovsky, Donetsk,

Leonova Lilia Alexandrovna

Donetsk National Technical University, Donetsk

Аннотация. В работе исследовано направление деятельности субъектов предпринимательства в сфере услуг, их эффективность во взаимосвязи с эффективностью территории региона, разработаны теоретико - методические подходы к определению влияния факторов, обеспечивающих возможности экономического развития субъекта, территории и региона в целом, предложено аналитическое выражение их зависимости и факторов взаимного влияния.

Ключевые слова: эффективность, сфера услуг, региональная экономика, субъекты предпринимательства, инновации, территория.

Abstract. The paper considers the activities of business entities in the service sector in relation to the territory of the region, develops theoretical and methodological approaches to determining the influence of factors that characterize the possibilities of economic development of the subject, territory and region as a whole, offers a formal expression of their dependence and factors of their mutual influence.

Keywords: efficiency, service sector, regional economy, business entities, innovations, territory.

DOI 10.54092/25420208_2021_9_60

Рецензент: Бессарабов Владислав Олегович - Кандидат экономических наук. ГО ВПО «ДонНУЭТ имени Михаила Туган-Барановского»

Эффективное функционирование субъектов предпринимательства сферы услуг в условиях региональной экономики, целью и результатом которой является их экономическое развитие, характеризуется процессом выявления и обобщения факторов, инновационного форсайт-прогнозирования, оказывающих воздействие на их результативность. Такие основы предполагают использование параметров, характеризующих эффективность функционирования предприятий, мультипликацию их влияния на показатели своей и смежных отраслей территории и региональной экономики в целом.

Одним из важнейших риск-элементов управления экономическим развитием субъектов предпринимательства сферы услуг являются формализованные процессы, которые на основе ключевых показателей эффективности позволяют формировать задачи их подразделений и сотрудников, обеспечивать форсайт-планирование работы, осуществлять мониторинг и экспертный контроль результатов, вносить соответствующие коррективы на основе современных инновационных технологий.

Уровень состояния сферы услуг *N*-го региона свидетельствует, что взаимосвязи субъектов предпринимательства и территории реализуются в условиях существования сложившейся структуры территориальной организации и базируются на принципах социально-общественной направленности и конкурентоспособности территории. Их функционирование и развитие неотъемлемы от экономического развития региона, так как конкретное предприятие находится в определенных пространственно – территориальных связующих отношениях. В таком положении субъект предпринимательства и его услуги выступают определенным потенциальным фактором социально-экономического развития региона, показателем соответствия регуляторной политики, предпринимательства и сферы услуг, индикатором взаимосвязи с инфраструктурой территории региона.

Деятельность предприятий, как субъектов хозяйствования, на различных экономических уровнях и отраслях сферы деятельности и предоставления услуг, разносторонняя и углубленная оценка ее эффективности неоднократно рассматривалась и нашла отражение в научных работах экономистов. Это ученые С.С. Абрамов [1], Т.В. Кириллова [2], С.Ф. Салихова и А.М. Губайдуллин [3], З.Г. Зайнашева и О.С. Мутраков [4], Д.Б. Кувалин [5] и др.

Учитывая, что деятельность субъектов предпринимательства, особенно малого и среднего изнеса, в значительной степени осуществляется в сфере услуг, исследование этой темы является актуальным. *Целью работы* является обобщение методических подходов на теоретической и праксеологической основе к определению эффективности сферы услуг как составляющей экономики территории региона.

Необходимость развития сферы услуг, создание благоприятных условий ведения предпринимательской деятельности в этой сфере, является неотъемлемой частью экономики региона, ее инновационной актив-составляющей. Как и в любом, традиционно функционирующем, секторе региональной экономики, в сфере услуг осуществляют свою деятельность крупные, средние и малые предприятия, кроме того функционируют такие субъекты как физические лица- частные предприниматели. Характерной особенностью сферы услуг является преобладающее большинство предприятий микро (семейного) и малого бизнеса. При этом на уровне территории непромышленные предприятия могут частично оказывать влияние на агентов поставщиков и потребителей, поскольку производители услуг являются самостоятельными и независимыми субъектами. Благодаря хорошо налаженному коммуникативному и финтех-взаимодействию с поставщиками и углубленной внутренней мотивации предприятия непромышленной сферы могут косвенным образом влиять на смежные с ними промышленные предприятия, создавая множественный эффект в других отраслях региональной экономики [6].

Субъекты предпринимательства заинтересованы уравнивать интересы между различными, задействованными в процессе деятельности ресурсами, они руководствуются общепринятыми нормами, приоритетами и представлениями о ценностях, имеют перед собой цели и программы по дальнейшему экономическому развитию и форсайт-прогнозированию территории региона.

Исследования [6;7] показали, что составляющими комплексного свойства «эффективность» являются:

- результативность – функция, отражающая степень соответствия сравниваемых полученных результатов их прогнозированным значениям;
- ресурсоемкость как цифровое выражение отношения финансового эффекта к затраченным на его достижение ресурсам всех видов (трудовым, материально-техническим, энергетическим, информационными, финансовыми, инновационным и т.п.);
- оперативность, определяемая расходом времени, необходимого для достижения цели функционирования по ее отдельным выше перечисленным аспектам с использованием цифровых и финансовых технологий в производстве, взаимодействии с системой банковского обслуживания, управляющими структурами;
- общественно-потребительская составляющая, которая представляет собой отношение субъективных целей к объективно существующим потребностям и ценностям территории региона.

Задача регионального управления требуют изучения всего комплекса отраслевых и территориальных интересов, разработки методологии и методов их

рационального сочетания. Методологической основой стратегического управления развитием региона должно быть оптимальное использование концепции инновационного направления развития, принципов снижения неопределенности и риска, обеспечения экономической безопасности, кластерных форм интеграции.

В сфере услуг, как и в других отраслях, предприятия имеют особенности и специфику, вытекающие из особенностей производственного процесса и характера услуг, финансирования, инновационных условий выполнения работ. Как основные понятия, характеризующие результаты работы, являются «эффективность», «эффект», «результативность», «экономическая результативность» производительность продуктивность, высокоэффективность.

На основе анализа научных и методических материалов можно утверждать, что функционирование предприятия, как процесса, с учетом характеристик территории региона осуществляется с целью создания конкурентоспособного на рынке продукта или услуг. Одним из условий такого процесса является соблюдение таких общих и специфических требований, которые смогут удовлетворить потребности и обеспечить на этой основе комплексное экономическое развитие субъектов предпринимательства и территории региона [8].

Выявленные факторы и условия охватывают виды деятельности и участие предприятий различных сфер хозяйствования. Факторы воздействия взаимосвязаны и должны учитываться во всей своей совокупности при планировании дальнейшего развития промышленной территории. Оценка факторов влияния является сложной и следующей задачей после анализа, и ее решение позволяет более объективно обосновать направления и средства улучшения ситуации относительно эффективного развития субъектов на территории региона (рис. 1).

В ходе исследования установлены характерные факторы [7]:

- для субъекта деятельности – фактор, имеющий название «операционная деятельность предприятия: систематическое создание продукции (услуг)», его характеристикой являются развитие технологических связей, наращивание внутреннего потенциала, развитие организационной и инновационной структуры;
- для региона и его территории – «ресурсный», «организационный» и «инновационный» факторы: обеспечение ресурсами, выявление и использование резервов, формирование инфраструктуры, кадровый потенциал», для которых характерным является совершенствование регионального управления, разработка и внедрение программ экономического развития.

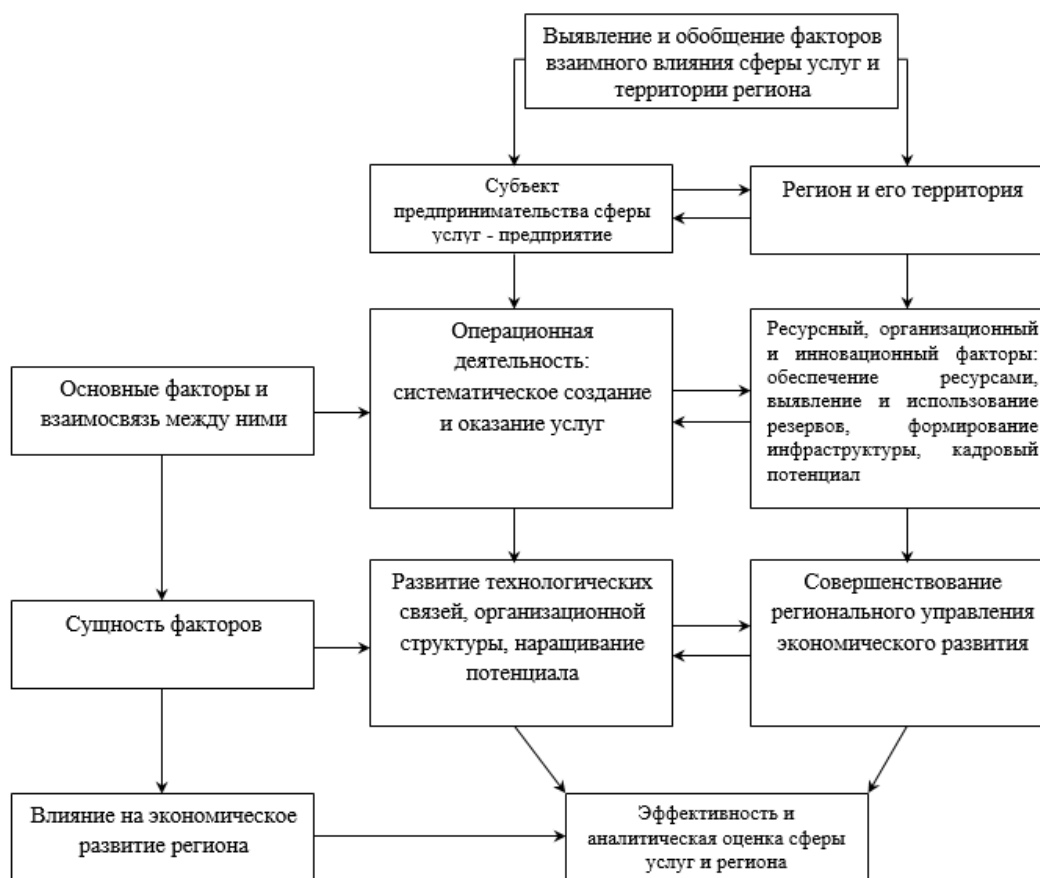


Рисунок 1. Влияние и обобщение факторов взаимного влияния субъекта предпринимательства сферы услуг на развитие региона

Рассмотрение каждого из приведенных потенциальных факторов выполняется в следующей методико-технологической последовательности:

- выявление, обобщение, отбор и группирование;
- предоставление характеристики; определение их влияния на формирование экономического развития.

Применение таких теоретико - методических рекомендаций требует правильного позиционирования управленческих мероприятий с акцентом на детерминированность процесса и участие персонала в инициировании и достижении показателей эффективности предприятия.

На основе проведенных исследований для создания практических условий эффективного функционирования субъектов предпринимательства на территории региона следует разработать подход к определению взаимного влияния факторов,

характеризующих возможности экономического развития субъекта и других контактных объектов территории региона.

На основании вышеизложенного можно сформулировать, что эффективность деятельности субъекта предпринимательства и территории региона рассматриваются как функция характерных для каждого из них факторов взаимного влияния, а именно эффективность территории региона; «операционная и инновационная деятельность» предприятия; «ресурсный» фактор или потенциал территории и субъекта предпринимательства;

Экономическая особенность этих факторов состоит в том, что каждый из них характеризует определенное направление экономического развития субъекта с целью выполнения и оказания услуг на территории региона, охватывает систематизированный перечень системных элементов, мероприятий и показателей.

Для раскрытия сущности теоретико-праксеологических подходов необходимо обозначить каждый фактор и определить его влияние на экономическое развитие региона:

1. Первый основополагающий фактор «операционная деятельность предприятия» характеризует деятельность субъекта в соответствии с установочными документами, преследующую формирование положительного финансового результата своей деятельности в качестве основной цели, либо не имеющей извлечение прибыли в качестве такой цели в соответствии с предметом и целями деятельности (неприбыльная организация), т. е. выполнение и оказание услуг.

Оценка влияния фактора «операционная и инновационная деятельность» основана на следующих принципах [7]:

поддержание и совершенствование договорных связей, направленных на постоянное стабильное урегулирование финансово-технологических и инновационных факторов, которые воздействуют на агентов и других участников процесса на территории региона при создании и предоставлении услуг;

наращивание внутреннего потенциала предприятия за счет использования собственных резервов в результате развития и совершенствования и модернизации видов услуг;

развитие управленческой и инновационной структуры, эффективности и форсайт-деятельности при условии выполнения и наращивания функций, связанных с созданием и реализацией услуг с помощью небанков, цифровых, интернет, финансовых и ИТ - технологий, которые обеспечивают эффективность деятельности субъекта предпринимательства.

2. Влияние «ресурсного» фактора территории региона и субъекта хозяйствования необходимо оценивать в экономической связи с формированием

системы хозяйствования и инфраструктуры территории, что в значительной степени обусловлено повышением предпринимательской активности действующих субъектов. В рамках тенденции использования ресурсов для удовлетворения социальных и экономических изменений необходима постоянная корректировка целей и диверсификация существующих видов продукции и услуг, расширение их ассортимента, улучшение качества [7].

Следует подчеркнуть, что воздействие таких факторов аналогично стимулирующей функции рычагов воздействия, что в современных условиях стимулирует заинтересованность территории в наиболее рациональном использовании своих ресурсов и наращивании внутреннего потенциала.

Исходя из того, что субъекты предпринимательства руководствуются мотивом удовлетворения социального запроса на продукцию и услуги, их целью является получение положительного результата, можно считать, что целесообразным будет выполнение только тех видов услуг, которые решают проблему насыщения данной территории на основе сформировавшегося спроса, повышают конкурентоспособность территории и являются основой экономического развития региона.

3. «Организационный» фактор территории учитывает инфраструктуру, систему ее внутренних и внешних, а также кластерных, связей, способствует совершенствованию организации производства, труда и управления, выбору организационно-правовой и организационно-экономической форм деятельности.

Для реализации этого фактора необходимо использование таких механизмов как использование бюджетов для планирования, сбалансированных систем управления компанией, мониторинга и контроля, управление ценовыми параметрами и структурой себестоимости, технологиями, определяющими текущую и будущую потенцированную стоимость продукции. Установление таких параметров, которые удовлетворяют интересам структурных подразделений и внешнего окружения, совершенствование структуры и формы внутренней аналитической оценки, обеспечение устойчивого развития будут способствовать совершенствованию управления экономикой региона.

Выводы. Экономическая эффективность субъектов предпринимательства сферы услуг на территории региона, базируется на рациональной направленности использования природных, промышленных и экономических ресурсов с целью экономического развития всех субъектов территории, оптимальном решении вопросов стабильного функционирования территории региона, адаптации предприятий к ее внутреннему и внешнему экономическому окружению.

В результате обобщения теоретических положений, раскрывающих сущность и особенности деятельности субъектов предпринимательства на территории региона,

можно считать, что разработка и использование теоретико - методических подходов будет способствовать экономическому развитию сферы услуг региона.

Библиографический список

1. Абрамов С.С. Оценка социально-экономической эффективности сферы услуг региона / С.С. Абрамов.– Научно-технические ведомости СПбГПУ: Экономические науки, 2011. –№3. – С.41-44.– Режим доступа. – <https://cyberleninka.ru/>
2. Кириллова Т.В. Применение матричных моделей для проведения анализа эффективности хозяйственной предприятий сферы услуг /Т.В. Кириллова // Материалы Всероссийской научно-практической конф.: Развитие сферы услуг: стратегии, инновации, компетенции», Новгород, 26 марта 2019 г., г. Н.Новгород - Нижний Новгород: Изд-во ННГУ, 2019. – С. 394-400.
3. Салихова С.Ф., Мутраков О.С., Губайдуллин А.М. Показатели экономической эффективности деятельности предприятий сферы услуг / С.Ф. Салихова, О.С. Мутраков, А.М. Губайдуллин. – Вестник УГНТУ: Наука, образование, экономика. Серия экономика. № 3 (17), 2016.– С. 42-48.
4. Зайнашева З.Г., Мутраков О.С. Особенности предпринимательской деятельности в сфере услуг / З.Г. Зайнашева, О.С. Мутраков. – Азимут научных исследований: экономика и управление. 2018. Т. 7. № 1(22). – С. 197-201.
5. Кувалин Д.Б. Экономическая политика и поведение предприятий: механизмы взаимного влияния / Д.Б. Кувалин. – Макс Пресс, 2009. – 320 с.
6. Balashova R. Improved territorial policy, as the direction of increase of efficiency of sphere of services (Совершенствование территориальной политики, как направление повышения эффективности сферы услуг) // European science review, «East West» Association for Advanced Studies and Higher Education GmbH. Vienna. №1-2. 2016, – pp. 201-203.
7. Балашова Р.И., Концептуальные подходы к повышению эффективности гостиничных предприятий на промышленной территории / Р.И. Балашова, Ю.Д. Баканова // Вестник Донецкого национального университета. Серия В: Экономика и право. – 2017. – №4. – С..13-22.
8. Кузьменко Л.М. Управление функционированием и развитием экономики региона: монография /Л.М. Кузьменко. – Донецк: ИЭП НАН Украины, 2004. – 284 с.

Экономика природопользования

УДК 33

Энхтүвшин Л., Ганчимэг Ж. Некоторые вопросы по планированию, контролю и анализу данных открытых рудников Some questions on planning, control and data analysis of open-pit mines

Энхтүвшин Л.

Цех связи, информации и технологической автоматизации, Предприятие Эрдэнэт
Орхон аймаг, Монголия
Доктор, доцент

Ганчимэг Ж.

Институт бизнеса,
Университет науки и технологий
город Улаанбаатар, Монголия

Enkhtyvshin L.

Communication, Information and Technological Automation Workshop, Erdenet Enterprise
Orkhon aimag, Mongolia
Doctor, Associate Professor

Ganchimeg J.

Institute of Business,
University of Science and Technology
Ulaanbaatar city, Mongolia

Аннотация. Для обеспечения равномерного технологического процесса обогащения руды обогатительной фабрики нужна подача руды с устойчивыми показателями без резких колебаний. Для этого необходимо начать с планирования добычи руды и постоянно отслеживать и анализировать качество подаваемой руды. Также необходимо управлять технологическим процессом обогащения руды в соответствии с физико-механическими свойствами, минеральным составом и минералогической структурой руды. Поэтому важна своевременная, оперативная обработка данных и генерирование отчетов для мониторинга и управления добычей руды, что в свою очередь оказывает прямое влияние на качество процесса извлечения и производства концентрата. Также существует потребность в прогнозе и расчёте оптимальных режимов технологических процессов на основе результатов анализа руды. Для решения этих проблем важно использовать программное обеспечение по сбору и обработке данных параметров руды и технологических процессов флотации, а также для оперативной подготовки расчётных данных и отчетов.

Ключевые слова: программное обеспечение, математическая модель, линейное программирование, оптимизация.

Abstract. To ensure a uniform technological process of ore beneficiation of a concentration plant, a supply of ore with stable indicators without sharp fluctuations is required. To do this, it is necessary to start with planning the ore extraction and constantly monitor and analyze the quality of the ore being supplied. It is also necessary to control the technological process of ore beneficiation in accordance with the physical and mechanical properties, mineral composition and mineralogical structure of the ore. Therefore, timely, prompt data processing and reporting is important for monitoring and managing ore mining, which in turn has a direct impact on the quality of the concentrate extraction and production process. There is also a need for forecasting and calculating the optimal modes of technological processes based on the results of ore analysis. To solve these problems, it is important to use software for the collection and processing of data on ore parameters and flotation technological processes, as well as for the prompt preparation of calculated data and reports.

Keywords: software, mathematical model, linear programming, optimization.

DOI 10.54092/25420208_2021_9_68

Рецензент: Тлехурай-Берзегова Лариса Талибовна - Доктор экономических наук, доцент. ФГБОУ ВО «Адыгейский государственный университет»

I. ВВЕДЕНИЕ

Один из способов достижения выше поставленных целей – использование специализированных программных обеспечений. На мировом рынке существуют различные программные обеспечения для планирования и управления горными работами, но стоимость и эксплуатационные расходы таких программ высоки.

“Предприятие Эрдэнэт” – горно-обогатительный комбинат в городе Эрдэнэт в Монголии, является одним из крупнейших горнорудных предприятий в Азии. “Предприятие Эрдэнэт” использует ряд программных обеспечений по планированию и управлению горных работ, автоматизированные системы по сбору данных различных технических и технологических процессов.

Целью данного исследования было изучение возможности создания и применения единого программного обеспечения по планированию, контролю и анализу данных рудника открытых работ, сбору исходных данных параметров руды и технологических процессов флотации, обработке и анализе результатов в условиях “Предприятия Эрдэнэт”.

Для достижения поставленной цели возникла необходимость оптимизировать некоторые процессы расчётов. Например, оптимизация расчёта шихты в соответствии с планом приёма и обработки руды, транспортировки и добычи руды. Для этого были проведены различные исследования по определению методологии, разработаны математические модели и написаны программные коды для нахождения оптимального решения.

II. ОПИСАНИЕ МЕТОДОЛОГИИ

Для решения поставленных задач возникла необходимость построения математической модели, определения оптимального режима, нахождения решения.

Линейное программирование — математическая дисциплина, посвящённая теории и методам решения экстремальных задач на множествах n -мерного векторного пространства, задаваемых системами линейных уравнений и неравенств. [1]

$$f(x) = \sum_{j=1}^n c_j x_j \rightarrow \max(\min) \quad (2.1)$$

$$\sum_{j=1}^n a_{ij} x_j = b_i, \quad i = \overline{1, m_1}; \quad m_1 < n$$

$$\sum_{j=1}^n a_{ij}x_j \leq b_i, \quad i = \overline{m_1+1, m_2} \quad (2.2)$$

$$\sum_{j=1}^n a_{ij}x_j \geq b_i, \quad i = \overline{m_2+1, m}$$

$$x_j \geq 0, \quad j = \overline{1, n_1}; \quad n_1 \leq n \quad (2.3)$$

Здесь $0 \leq m_1 \leq m_2 \leq m$, a_{ij} , c_j , b_i - заданные действительные числа, (2.1) - целевая функция, (2.2) - ограничения, (2.3) – условие, при которых переменные не отрицательны.

Существуют различные способы нахождения решений задач линейного программирования. В настоящее время исследователи широко используют программное обеспечение Matlab для нахождения решений задач линейного программирования.

Matlab - это высокопроизводительный программный пакет для математических расчетов и моделирования. Программа имеет сотни стандартных функций или команд для использования в различных технических расчетах, графике и анимаций. В большинстве этих команд используются новейшие методы и алгоритмы. [2]

В Matlab задачи линейного программирования могут быть решены с помощью таких команд, как linprog, simple и bintprog. Команда linprog имеет большое преимущество в том, что касается общих задач линейного программирования, поэтому ее часто используют на практике. [2]

III. ОСНОВНАЯ ЧАСТЬ

а) Количество и качество подаваемой руды на ОФ¹ должна соответствовать заданному плану. Если считать, что за одну смену ОФ сможет принять руду в количестве Q , с содержанием меди a , то общее количество меди в руде будет

$$b = Q \cdot a \quad (3.1).$$

Для добычи Q руды требуется n экскаваторов. Тогда

¹ ОФ – Обогажительная фабрика

$$b = \sum_{j=0}^n q_j \cdot a_j \quad (3.2).$$

Здесь:

q_j ($j = 1 \div n$) – количество добываемой руды j -ого экскаватора,

a_j ($j = 1 \div n$) – содержание меди в добываемой руде j -ого экскаватора.

С другой стороны затраты добываемой руды j -ого экскаватора будут c_j ($j = 1 \div n$). В зависимости от технических характеристик экскаватора за смену минимальное количество добытой руды будет p_1 , а максимальное p_2 . Тогда требуется составить такой план, при котором будут удовлетворены план приёма ОФ и суммарные затраты на перевозку руды будут минимальны.

Учитывая условие неотрицательности объёмов перевозок, математическую модель задачи можно записать так:

$$f(x) = \sum_{j=0}^n c_j \cdot q_j \rightarrow \min \quad (3.3)$$

$$Q \cdot a = \sum_{j=0}^n q_j \cdot a_j \quad (3.4)$$

$$p_1 \leq q_j \leq p_2 \quad (3.5).$$

Считаем, что переменные Q , a , n , p_1 , p_2 , c_j ($j = 1 \div n$), a_j ($j = 1 \div n$) математической модели известны. Здесь: Q – приём руды ОФ за смену, a – планируемое содержание меди в руде, подаваемой ОФ, n , p_1 , p_2 зависят от технических характеристик используемой техники.

Из описанной математической модели видно, как много зависит от того, как определена a_j .

б) Рассмотрим следующий пример определения a_j ($j = 1 \div n$). Предположим, что на поверхности рудного карьера сформирована прямоугольная сетка размером $m \times m$. Тогда в центре каждой прямоугольной сетки пробуем скважину, откуда на глубине h возьмём пробу руды и определим содержание меди в пробе. Таким образом определим содержание меди в трехмерном $m \times m \times h$ блоке-параллелепипеде. По мере увеличения размера этих трехмерных блоков способность одной пробы представлять весь блок ухудшается. Исходя из технических и экономических ресурсов на практике возможность изготовления большого количества опытных проб ограничено. В

зависимости от имеющихся ресурсов, желательно использовать аналитические методы для более точного определения содержания меди в каждом блоке руды.

Если предположить, что распределение содержания меди между центральными точками трехмерных $m \times m \times h$ блоков линейное, то можно определить любое значение содержания меди в блоке в точке k .

Для этого воспользуемся методом нахождения уравнения прямой, проходящей через две точки на плоскости. Уравнение прямой, проходящей через точки (x_1, y_1) , (x_2, y_2) будет

$$\frac{y-y_1}{y_2-y_1} = \frac{x-x_1}{x_2-x_1} \quad (3.6)$$

или

$$y = \frac{(x - x_1)(y_2 - y_1)}{x_2 - x_1} + y_1 \quad (3.7).$$

Это интерполяция многочлена Лагранжа при $n = 1$. Тогда содержание меди в точках параллелепипеда можно найти в зависимости содержания меди в соседних блоках.

Предположим, что вокруг блока №0 расположены 8 блоков с номерами №1, №2, №3, №4, №5, №6, №7, №8, где расстояние между центральными точками соседних блоков $m = 8$ метров, и известны содержание меди в центральных точках (Таблица 1).

Таблица 1

Анализы проб в центральных точках блоков.

Номер блока	№0	№1	№2	№3	№4
Содержание меди Cu, %	0.350	0.500	0.300	0.455	0.578
Номер блока	№5	№6	№7	№8	-
Содержание меди Cu, %	0.645	0.596	0.560	0.370	-

Также предположим, что каждую линию в блоке №0, проведенных от центра блока №0 до центра соседних блоков, разделили на 8 равных частей. Тогда в таблицах 2.1 и 2.2 показаны расчётные данные содержания меди в точках деления блока №0.

Таблица 2.1

Расчётные данные содержания меди в точках деления блока №0.

Номер блока	Содержание меди Cu в центральных точках блоков, %	Расстояние от центральной точки блока №0 до центральной точки соседнего блока, метр				
		0.8	1.6	2.4	3.2	4.0
1	0.500	0.350	0.367	0.383	0.400	0.417
2	0.300	0.350	0.344	0.339	0.333	0.328
3	0.455	0.350	0.362	0.373	0.385	0.397
4	0.578	0.350	0.375	0.401	0.426	0.451
5	0.645	0.350	0.383	0.416	0.448	0.481
6	0.596	0.350	0.377	0.405	0.432	0.459
7	0.560	0.350	0.373	0.397	0.420	0.443
8	0.370	0.350	0.352	0.354	0.357	0.359
Среднее содержание меди, %		0.400	0.504	0.608	0.711	0.815
Среднее содержание меди Cu блока №0, %		0.608				

Таблица 2.2

Расчётные данные содержания меди в точках деления блока №0.

Номер блока	Содержание меди Cu в центральных точках блоков, %	Расстояние от центральной точки блока №0 до центральной точки соседнего блока, метр				
		4.8	5.6	6.4	7.2	8.0
1	0.500	0.433	0.450	0.467	0.483	0.500
2	0.300	0.322	0.317	0.311	0.306	0.300
3	0.455	0.408	0.420	0.432	0.443	0.455
4	0.578	0.477	0.502	0.527	0.553	0.578
5	0.645	0.514	0.547	0.579	0.612	0.645
6	0.596	0.487	0.514	0.541	0.569	0.596
7	0.560	0.467	0.490	0.513	0.537	0.560
8	0.370	0.361	0.363	0.366	0.368	0.370
Среднее содержание меди, %		0.919	1.023	1.126	1.230	1.334

Тогда расчётное среднее содержание меди в блоке №0 будет равно 0.608%. В данном примере количество соседних блоков было 8. Максимальное количество соседних блоков может быть 26. Также, в данном примере прямую, соединяющую центральные точки соседних блоков с блоком №0, разделили на 9 равных отрезков. Эту прямую можно разделить на большее количество.

в) Определяем эффективность усреднения руды по формуле В.А.Шевелева [3]:

$$\eta = 1 - \frac{\sigma_n}{\sigma_y} \quad (3.8)$$

здесь σ_n - стандартное отклонение качества неусредненной руды, т.е. расчётное содержание меди в подаваемой руде,

σ_y - стандартное отклонение качества усредненной руды, т.е. анализ содержания меди в подаваемой руде.

При $\eta = [0,6 - 0,7]$ эффективность усреднения руды считается нормальной.

г) Проанализируем колебание содержания меди в руде:

Таблица 3.1

Данные переработки руды.

Год	Стандартное отклонение содержания меди в руде, σ	Стандартное отклонение извлечения меди в концентрате, σ
	1	2
2013	0.02696	1.51179
2014	0.02687	1.92816
2015	0.02465	1.94642
2016	0.02604	1.08424
2017	0.01919	1.05714
2018	0.01906	0.96731

Таблица 3.2

Данные переработки руды.

Год	Стандартное отклонение качества концентрата, σ	Стандартное отклонение содержания меди в хвостах, σ	Стандартное отклонение выхода концентрата, σ
	3	4	5
2013	0.51549	0.02475	0.11882
2014	0.51892	0.02549	0.13587
2015	0.36015	0.02307	0.11558
2016	0.31687	0.02609	0.11297
2017	0.27412	0.00533	0.08095
2018	0.33377	0.00467	0.08692

Стандартное отклонение содержания меди в руде в 2018 году составило 0.01906, что на 26.8 процента меньше по сравнению с 2016 годом и на 0.68 процента меньше по сравнению с 2017 годом.

Результаты корреляционного анализа содержания меди в руде представлены в таблице 4.

Таблица 4

Корреляционный анализ содержания меди в руде.

Наименование показателя	Стандартное отклонение содержания меди в руде	
	Коэффициент корреляции, r	Теснота связи
Отклонение извлечения меди в концентрате	0.64862	умеренная
Отклонение качества концентрата	0.72045	умеренная
Отклонение содержания меди в хвостах	0.98522	высокая
Отклонение выхода концентрата	0.94056	высокая
<i>Пояснение тесноты связи</i>		
<i>При коэффициенте корреляции $r < 0.5$ – слабая, при коэффициенте корреляции $0.5 < r < 0.75$ – умеренная, при коэффициенте корреляции $0.75 < r < 0.9$ – заметная, при коэффициенте корреляции $0.9 < r < 1.0$ высокая теснота связи.</i>		

Как видно из приведенных выше таблиц, устойчивое, без резких колебаний содержание меди в руде обеспечивает стабильную регулировку технологического процесса обогатительной фабрики:

- теснота связи стандартного отклонения содержания меди в руде и отклонения извлечения меди в концентрате умеренная,
- теснота связи стандартного отклонения содержания меди в руде и отклонения качества концентрата умеренная,
- теснота связи стандартного отклонения содержания меди в руде и отклонения содержания меди в хвостах высокая,
- теснота связи стандартного отклонения содержания меди в руде и отклонения выхода концентрата высокая.

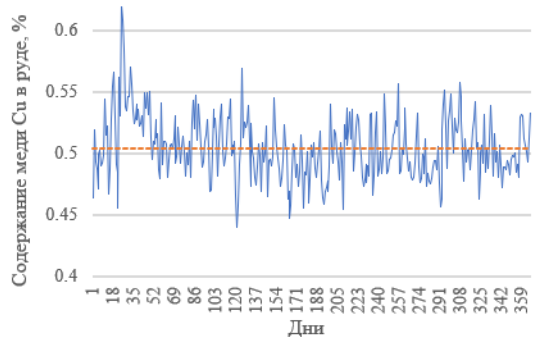


График 1: *График содержания меди Si в руде за 2016 год.*

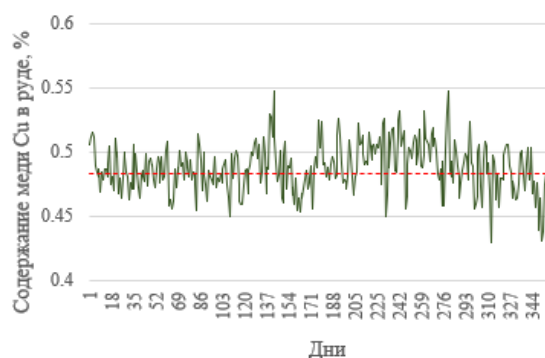


График 2: *График содержания меди Si в руде за 2017 год.*

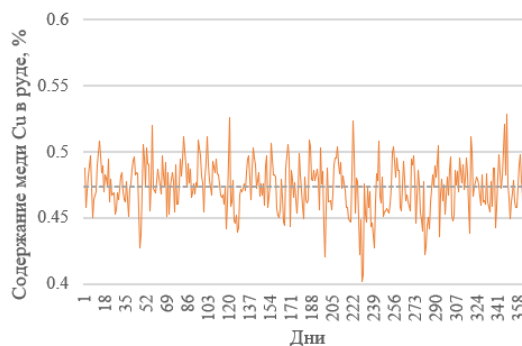


График 3: *График содержания меди Si в руде за 2018 год.*

Стандартное отклонение содержания меди в руде в 2018 году составляет 0.01906, что на 0.68% меньше, чем в 2017 году, когда оно составляло 0.01919, это указывает на то, что колебания содержания меди в руде уменьшились.

д) Рассмотрим анализы выхода концентрата:

Таблица 5.1

Данные выхода концентрата.

Год	Расчётные данные технологического баланса			
	σ	Разница, +/-	Выход, %	Содержание меди Cu в руде, %
	1	2	3	4
2013	0.02696		2.0071	0.530
2014	0.02687	-0.00009	2.0009	0.526
2015	0.02465	-0.00222	1.9198	0.516
2016	0.02604	0.00139	1.9681	0.510
2017	0.01919	-0.00685	1.8719	0.495
2018	0.01906	-0.00013	1.8340	0.480

Здесь:

- 1 – стандартное отклонение содержания меди Cu в руде, σ ;
 2 – разница стандартного отклонения содержания меди в руде в сравнении с предыдущим годом, + / -;
 3 – среднее значение выхода концентрата, %;
 4 – содержание меди в руде, %.

Таблица 5.2

Данные выхода концентрата.

Год	Данные товарного баланса				
	Выход, %	γ	Q	ε	Содержание меди Cu в концентрате, β
	5	6	7	8	9
2013	1.9689	-	-	86.30	23.32
2014	2.0225	-	-	86.55	23.03
2015	1.9495	-	-	88.22	23.35
2016	1.9207	598 517.00	31 180 000	87.56	23.25
2017	1.8918	595 095.88	31 438 000	89.28	23.36
2018	1.8611	585 979.68	31 520 000	89.49	23.08

Здесь:

- 5 – среднее значение выхода концентрата, %;
 6 – выход концентрата (сухой вес), тн, γ ;
 7 – переработка руды (сухой вес), тн, Q ;

8 – извлечение меди, %, ε ;

9 – содержание меди в руде, %, β .

Анализ показателей 2018 года по сравнению с предыдущим годом:

- стандартное отклонение содержания меди в руде уменьшилось на 0.00013 или 0.68%,

- извлечение меди увеличилось на 0.21 или 0.24%.

Выход концентрата определяется по следующей формуле:

$$\gamma_{cu} = \frac{\varepsilon_{cu} \cdot \alpha_{cu}}{\beta_{cu}} \quad (3.9)$$

Где:

γ_{cu} – выход концентрата,

ε_{cu} – извлечение меди,

α_{cu} – содержание меди Cu в руде,

β_{cu} – содержание меди Cu в концентрате.

Если предположить, что технология обогатительной фабрики в 2018 году не менялась, но изменилось содержание руды, то расчётный выход концентрата можно рассчитать по формуле (3.9):

$$\gamma_{cu \text{ 2018 расчётное}} = \frac{\varepsilon_{cu \text{ 2017}} \cdot \alpha_{cu \text{ 2018}}}{\beta_{cu \text{ 2017}}} = 1.8345.$$

Фактический выход концентрата в 2018 году был $\gamma_{cu \text{ 2018 фактическое}} = 1.8611$, тогда разница расчётного и фактического выходов концентратов будет равна

$$\gamma_{cu \text{ 2018 расчётное}} - \gamma_{cu \text{ 2018 фактическое}} = -0.0266.$$

Из выше сделанных расчётов видно, что фактический выход концентрата больше расчётного на 1.43 процента.

Воспроизведём вышесделанные расчёты на данных 2013-2018 годов. Данные, использованные в расчётах, и результаты расчётов показаны в таблицах 6.1, 6.2, 6.3.

Таблица 6.1

Данные выхода концентрата.

Год	Данные товарного баланса		
	Среднее значение выхода концентрата, %	Извлечение меди Cu, % ε	Содержание меди Cu в концентрате, β
2013	1.9689	86.30	23.32
2014	2.0225	86.55	23.03
2015	1.9495	88.22	23.35
2016	1.9207	87.56	23.15
2017	1.8918	89.28	23.36
2018	1.8611	89.49	23.08

Таблица 6.2

Данные выхода концентрата.

Год	Данные товарного баланса	
	Содержание меди Cu в руде, %	Среднее значение выхода концентрата, %
2013	0.530	1.9689
2014	0.526	2.0225
2015	0.516	1.9495
2016	0.510	1.9207
2017	0.495	1.8918
2018	0.480	1.8341

Таблица 6.3

Данные выхода концентрата.

Год	Расчётные данные технологического баланса	Разница расчётного и среднего значения фактического выхода концентратов, +/-
	Среднее значение выхода концентрата, %	
2013	1.9904	1.9689
2014	1.9466	0.0215
2015	1.9392	-0.0759
2016	1.9269	-0.0103
2017	1.8642	0.0062
2018	1.8345	-0.0276

Разницы расчётного и среднего значений фактического выхода концентратов в 2014, 2015, 2017 годах имеют отрицательные значения. Из этого можно сделать вывод, что именно в этих годах проводились какие-либо значительные улучшения в технико-технологических аспектах производства.

е) Для создания и применения единого программного обеспечения по планированию, контролю и анализу данных рудника открытых работ инженерами “Предприятия Эрдэнэт” было разработано программное обеспечение MAS. Программа MAS разрабатывалась, внедрялась в производственную эксплуатацию, и модернизировалась в 2017-2018 годах. В программе использованы следующие данные:

- база данных производственного технологического процесса,
- база данных системы “Питрам”,
- 13 видов геологических карт распределения минералов и элементов,
- «Карта Малютина» (доцент МГУ Ю.А.Малютин), показывающая тип и структуру минералов на горизонтах месторождения Эрдэнэтийн Овоо, проведенная для изучения рудных минералов в 2002 году (обработка информации о минералах меди важно для оценки ценных и токсичных элементов, содержащихся в минерале),
- база данных программы Micromine для расчёта ресурсов руды, планирования, проектирования и моделирования блоков взрывных работ,
- база данных GEOBank,
- методология и алгоритмы программы “Цифровая модель месторождения ЦММ”,
- библиотечные файлы программы Matlab,
- месячный, недельный, сменный план работы рудника и обогатительной фабрики,
- схема потока данных производственных отделов и цехов.

Ниже показаны некоторые формы и отчёты программы MAS.

ИЛ УУРХАЙГААС ХҮДЭР АЧИХ ГЕОЛОГИЙН ДААЛГАВАР

The screenshot displays the MAS software interface, which is used for ore processing calculations. It features several panels and tables:

- Top Panel:** Includes a date selector (5/20/2018), a language dropdown (Гарга), and buttons for saving and loading data.
- Left Panel (Төлөвлөгөө):** Contains a table for inputting data, with columns for 'Хүдэр' (Ore) and 'Сод.Сү.' (Concentration). It lists various ore types (ЭКГ №12 to ЭКГ №25) and their concentrations.
- Center Panel (Тооцоолол):** A large table for calculations, with columns for 'Хүдэр', 'Сод.Сү.', 'Гориз', and 'Блок'. It shows calculated values for different ore types and blocks.
- Right Panel (Шийд):** A table for results, with columns for 'Хүдэр', 'Сод.Сү.', 'Объем', and 'Сод.Сү. %'. It displays calculated values for different ore types and blocks.
- Bottom Panel (Рейсийн тоо):** A table for results, with columns for 'ККД', 'КСИ', and 'Total'. It shows calculated values for different ore types and blocks.

The interface also includes a 'Grand Total' section at the bottom right, showing the overall results of the calculations.

Рисунок 1: Форма расчёта шихтовки руды за смену.

НОО «Профессиональная наука» использует Creative Commons Attribution (CC BY 4.0): лицензию на опубликованные материалы - <https://creativecommons.org/licenses/by/4.0/deed.ru>

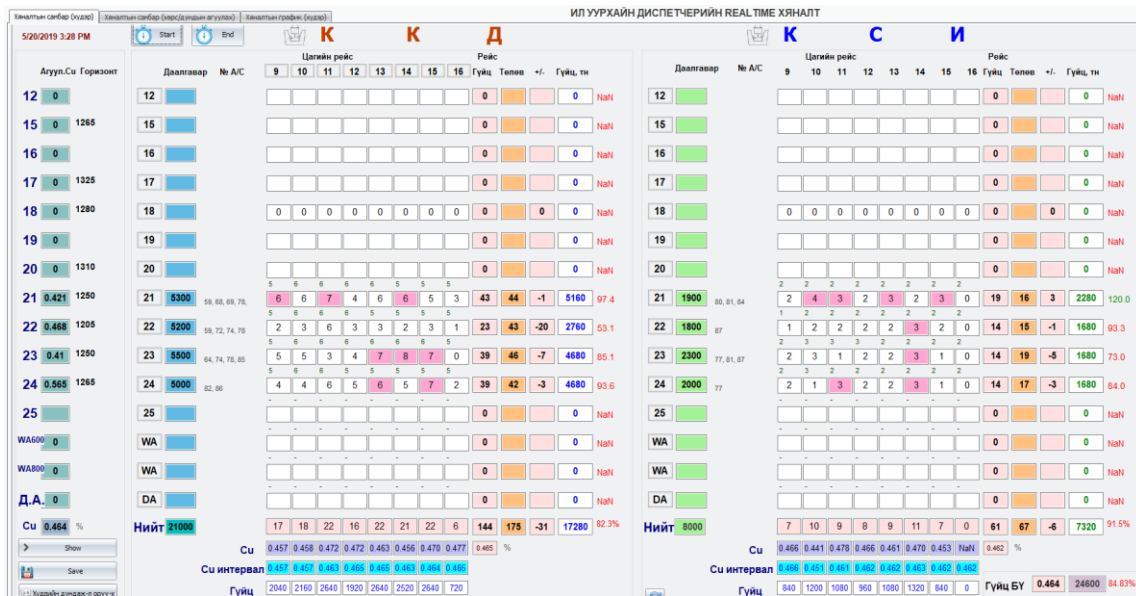


Рисунок 2: Форма мониторинга содержания меди Cu в добываемой руде, выполнение плана и т.д.. Количество рейсов автосамосвалов можно вводить вручную. В данной форме количество рейсов автосамосвалов экспортируются автоматически из базы данных системы Питрам.

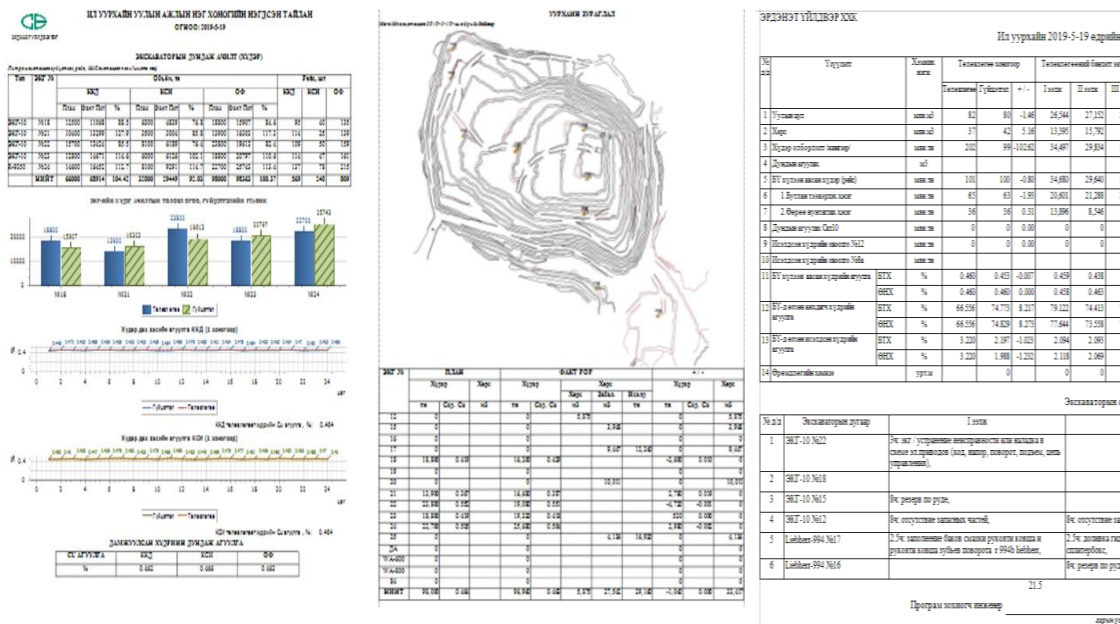


Рисунок 3: Отчётные формы горных работ. Средняя загрузка экскаватора, план загрузки руды и график работы. График содержания меди в руде. Контур рудника создан из более 20000 точек контура системы Micromine, который обновляется каждый раз при получении отчёта.

IV. ВЫВОДЫ

1) Программа MAS производит сбор и обработку данных параметров руды и технологических процессов флотации, а также производит некоторые оптимизационные расчёты. В задачу программы MAS входят:

- оптимизация шихтовки руды и отгрузки руды из рудника;
- контроль содержания руды, передаваемой с рудника на обогатительную фабрику;
- предоставление информации о минеральных и минералогических составах и свойствах руды для управления производственным процессом;
- получение информации из карты блоков рудника для исследования;
- возможность учёта количества и содержания окисленной и несбалансированной руды;
- выполнение плана производства;
- произведение расчётов с использованием базы данных системы Питрам и Macromine;
- формирование единных отчётных форм горных работ.

2) Стандартное отклонение содержания меди Cu в руде в 2018 году составляет 0.01906, что на 0.68 процента меньше, чем в 2017 году, что указывает на уменьшение колебания содержания меди Cu в руде.

3) В 2018 году отклонение выпуска концентратов увеличилось на 0.00597 единиц (7.37%), что указывает в том числе на необходимость в дальнейшем детальном изучении влияния факторов на технологические процессы обогатительной фабрики.

Библиографический список

1. Р. Энхбат, “Оптимизация-2 (линейное программирование).” г. Улаанбаатар, 2009, стр. 1-4.
2. Б. Ууганбаяр, Д. Ариун-Эрдэнэ, “Использование Matlab”, 3 издание, г. Улаанбаатар хот, 2019, стр.6, 80.
3. В.А. Шевелев, “Определение эффективности усреднения руды на буферно-усреднительных складах”, 2014.
4. John H. Mathews, Kurtis D.Fink. “Numerical methods using MATLAB. Third edition”. 1999 он.
5. “Система MAS для планирования и анализа рудника”. Л.Энтүвшин. 2018.

Экономика труда

УДК 316.46

Кудрявцева М.В. Лидерство руководителей как фактор повышения эффективности деятельности современных компаний

Leadership of managers as a factor in improving the efficiency of modern companies

Кудрявцева Мария Викторовна

Старший преподаватель кафедры социальной работы и права
Санкт-Петербургский государственный университет
промышленных технологий и дизайна,
Санкт-Петербург

Kudryavtseva Maria Viktorovna

Senior Lecturer of the Department of social work and law
Saint Petersburg University of industrial technology and design,
Saint Petersburg

Аннотация. В статье рассматриваются некоторые тенденции, характерные для современных рыночных отношений. Подчеркивается роль процессов цифровизации, внедрения инноваций и других глобальных изменений, которые влияют на рынок труда и существенно преобразовывают современные компании и организации. Отмечается роль руководителей всех уровней в обеспечении конкурентоспособности компании и эффективности процессов управления человеческими ресурсами в условиях новой действительности. В контексте рассматриваемой проблемы особое значение приобретает способность руководителя быть лидером в своем коллективе, в своей компании. В статье рассматриваются некоторые аспекты лидерства и его потенциал в вопросах повышения эффективности деятельности современных компаний.

Ключевые слова: лидерство, руководители, эффективность, цифровизация, изменения, человеческие ресурсы, управление.

Abstract. The article examines some of the trends characteristic of modern market relations. The role of digitalization processes, innovation and other global changes that affect the labor market and significantly transform modern companies and organizations is emphasized. The role of managers at all levels in ensuring the competitiveness of the company and the effectiveness of human resource management processes in the new reality is noted. In the context of the problem under consideration, the ability of a leader to be a leader in his team, in his company is of particular importance. The article examines some aspects of leadership and its potential in improving the efficiency of modern companies.

Keywords: leadership, leaders, efficiency, digitalization, change, human resources, management.

DOI 10.54092/25420208_2021_9_83

Рецензент: Тлехурай-Берзегова Лариса Талибовна - Доктор экономических наук, доцент. ФГБОУ ВО «Адыгейский государственный университет»

В современных условиях ускоренного инновационного и научно-технологического развития происходят фундаментальные изменения рынка труда. Автоматизация многих рабочих процессов, внедрение систем искусственного

интеллекта, роботизация существенно преобразовывают компании и организации. Нарастающие темпы этих изменений обуславливают жесткую конкурентность на современной рыночной арене, повышение требований к качеству человеческих ресурсов, необходимость изменения подходов к управлению персоналом.

В условиях глобальных трансформаций, инноваций, новых бизнес-моделей любая компания заинтересована в привлечении и удержании высококачественных человеческих ресурсов, в привлечении клиентов и партнеров с перспективой долгосрочных и эффективных деловых взаимоотношений. При этом ускоренно возрастают требования к специалистам нового времени, которые должны адаптироваться к рыночным изменениям и подстраиваться под них.

По мнению отечественных исследователей, для современно рынка труда свойственны такие процессы, как:

- «падение спроса в низкоквалифицированной рабочей силе;
- появление особого «страта» сверхкомпетентных работников, обеспечивающих надлежащее функционирование сложной и дорогостоящей техники; уменьшение количества лиц, занятых на производстве, и расширение персонала, чьи трудовые обязанности связаны с конструированием, проектированием, обслуживанием, продвижением;
- поощрение работников, умеющих обращаться с новейшими устройствами и приборами и владеющих иностранным языком (как правило, английским) в рамках полученной профессии;
- активный поиск руководителей, способных выстраивать коллективную деятельность, использовать человеческие и неодушевленные (материальные, хронологические и т.д.) ресурсы с максимально возможным результатом;
- динамичное изменение спроса на навыки, компетенции и личностно-профессиональный опыт» [1, с. 286].

Особую роль в организации и управлении бизнес-процессами компании в условиях цифровой трансформации играют руководители всех уровней. Именно на них возлагается ключевая ответственность за обеспечение конкурентоспособности компании, оптимизацию внутренних организационных процессов, постоянное повышение их эффективности с учетом происходящих социально-экономических изменений. При этом особое значение отводится способности руководителя успешно взаимодействовать с коллективом, работать в команде, поскольку грамотное управление человеческими ресурсами является важнейшим фактором повышения конкурентоспособности компаний в эпоху цифровизации.

В отечественных научно-исследовательских работах подчеркивается, что «сегодня модель бизнеса складывается в тесном переплетении информационных

технологий и человеческих ресурсов. В основе осуществления бизнес – целей лежит индивидуальность каждого сотрудника и его сопричастность к компании. Каждый потенциал работника направлен на изменения и при этом на устойчивую приверженность принципам и ценностям компании» [2, с. 75].

Вне сомнений, эффективное руководство признано ключом к успеху любой компании. Умение руководителя формировать команды и управлять ими, умение организовывать слаженную работу своих сотрудников с учетом их индивидуальных качеств и способностей позволяет с наибольшей результативностью достигать поставленные компанией цели и задачи.

В контексте рассматриваемой проблемы особое значение приобретает способность руководителя быть лидером в своем коллективе, в своей компании (в зависимости от уровня руководства – низового, среднего или высшего звена). Лидеры, занимающие управленческие должности, обладают ценным потенциалом воодушевлять своих последователей к творческой деятельности; мобилизовать их ресурсы, устремляя к общим, но значимым для каждого сотрудника целям; повышать производительность труда.

Лидерство – одно из самых сложных и многогранных явлений, которое широко изучалось в области зарубежных социально-психологических и экономических наук на протяжении всего XX столетия. В современном быстроизменяющемся мире лидерство приобретает особое значение, в том числе в работе с молодыми поколениями. Анализ научной литературы показал, что «некоторые руководители убеждены в том, что прежние методы мотивации не работают при руководстве молодыми специалистами, и лидерство играет в этом особую роль. Воодушевленный глава компании способен зарядить всю команду энергией. Яркими примерами являются Марк Цукерберг из Facebook и Стив Джобс из Apple. Они не просто управляют сотрудниками компании. Они дают каждому почувствовать свою значимость и роль в изменениях, которые будут происходить в их компаниях» [3, с. 241].

По мнению зарубежных исследователей, лидерство и менеджмент обладают важными сходствами, поскольку и в первом, и во втором случае происходит взаимодействие с людьми и влияние на них для достижения определенных целей. В некотором роде это две отдельные, но дополняющие друг друга системы действий. Для устойчивого успеха компания нуждается как в менеджменте (планирование, организация, координация, контроль с учетом жестких временных сроков), так и в лидерстве, которое более открыто в своих идеях, обладает большей гибкостью, характеризуется вовлеченностью в командную работу, стремиться к долгосрочным целям и глобальным изменениям [4].

Большинство современных компаний испытывают определенные трудности от избытка менеджмента и нехватки лидерства и, соответственно, нуждаются в развитии способности к лидерству у руководителей всех уровней. Выдающиеся лидерские качества приносят изменения за счет поддержки сотрудников, инициативности в решении проблем и настойчивости в решении проблем [5].

В современных условиях интенсивных изменений популярность приобретают трансформационные теории лидерства. В теории трансформационного лидерства лидеры поощряют, вдохновляют и мотивируют своих последователей [6]. Данная теория используется, когда компания нуждается в обновлении, претерпевает значительные изменения или нуждается в поиске нового направления своего развития, что особенно актуально в условиях быстроразвивающейся технологической отрасли, где важно проявлять гибкость и инновационность для обеспечения постоянной конкурентоспособности компании. Яркими примерами трансформирующих лидеров современного мира являются Стив Джобс и Билл Гейтс [7].

Сегодня существует многообразие моделей лидерства и вариантов лидерского поведения, однако необходимо подчеркнуть, что эффективных лидеров разных уровней управления объединяет высокий уровень развития эмоционального интеллекта. Руководитель, который проявляет высокие интеллектуальные способности, генерирует идеи, владеет профессиональной компетентностью, но не обладает развитым эмоциональным интеллектом, не будет способен оптимально использовать весь потенциал лидерства.

Составляющие эмоционального интеллекта лидера, по мнению американского исследователя Дэниела Гоулмана, можно представить следующим образом:

- самосознание – способность принимать свои сильные и слабые стороны, ценности, мотивы;
- самоконтроль – способность контролировать или направлять в плодотворное русло разрушительные импульсы и эмоции;
- мотивация – желание работать ради самого процесса;
- эмпатия – способность понимать эмоциональные состояния других людей;
- социальные навыки – умение налаживать и управлять отношениями с другими людьми [8, с. 9].

Зарубежные исследования показали, что, когда высшее руководство компании обладает развитым эмоциональным интеллектом и использует пять вышеобозначенных навыков, ежегодные показатели прибыли всех подразделений на 20 % превышают запланированные [8].

Итак, ускорение темпов научно-технологических изменений, цифровая трансформация, внедрение инноваций в социально-экономическую сферу, усиление

конкуренции на рыночной арене и многие другие факторы предопределяют существенные изменения в современном деловом мире. Это стимулирует компании искать эффективные методы управления внутренними процессами организации и человеческими ресурсами, которые помогут сохранить и приумножить конкурентоспособность. Лидерство становится важным инструментом повышения производительности труда и определяющим фактором успеха современных компаний в новых социально-экономических условиях.

Библиографический список

1. Сергеева М.Г. Подготовка конкурентоспособного специалиста в условиях цифровизации образования // Проблемы современного педагогического образования. – 2020. – № 66-2. – С. 286-290.
2. Сураева М.О., Кучерявенко Д.М. Тенденция развития корпоративного управления на предприятиях в условиях инновационной трансформации // Научный результат. Экономические исследования. – 2020. – Т. 6. – № 4. – С. 71-79.
3. Казначеева С.Н., Челнокова Е.А. К вопросу о формировании лидерства // Инновационная экономика: перспективы развития и совершенствования. – 2019. – № 2 (36). – С. 39-245.
4. Northouse P.G. Leadership theory and practice (7th ed.). Thousand Oaks, CA: SAGE. – 2016. – 494 p.
5. Aarons G.A., Green A.E., Trott E., Willging C.E., Torres E.M., Ehrhart M.G., Roesch S.C. The roles of system and organizational leadership in system-wide evidence-based intervention sustainment: A mixed-method study // Administration and Policy in Mental Health. – 2016. – № 43(6). – P. 991-1008.
6. Flynn SI. Transformational and Transactional leadership // Great Neck Publishing. – 2019. – 6 p.
7. Benmira S, Agboola M. Evolution of leadership theory // BMJ Leader. – 2021. – P. 3-5.
8. Лидерство / Пер. с англ. – 3-е изд. – М. : Альпина Пабlishер, 2021. – 224 С.

Экономическая теория

УДК 33

Луговая Н. Г. Страхование, новые тренды и динамика развития Insurance, new trends and development dynamics

Луговая Н. Г.,

Приднестровский государственный университет им. Т. Г. Шевченко

Lugovaya N.G.,

Transnistrian State University named after T. G. Shevchenko

Аннотация. В статье рассматриваются современные тенденции страхования с учетом новых вызовов и возможностей цифровой экономики. Современные технологии становятся доступными для более широкого круга лиц, и теперь потребители требуют удобства, адаптивности и высоких скоростей в предоставлении услуг.

Ключевые слова: страхование, цифровая экономика, страховой продукт, инновации, технологические компании.

Abstract. The article considers main current trends in insurance taking into account new challenges and opportunities of digital economy. New technologies are becoming available to a wider range of people, and now consumes demand convenience, adaptability and high speeds in the provision of services.

Keywords: insurance, digital economy, insurance product, innovation, technological companies.

DOI 10.54092/25420208_2021_9_88

Рецензент: Тлехурай-Берзегова Лариса Талибовна - Доктор экономических наук, доцент. ФГБОУ ВО «Адыгейский государственный университет»

Распространение и совершенствование цифровых технологий влияет на развитие производственных отношений, структуру экономики и образование. Определяет новые требования к коммуникациям, информационным системам и сервисам.

В современных условиях динамичное развитие рынков и сфер деятельности вряд ли возможно без развитых платформ, технологий, институциональной и инфраструктурной сред.

Процесс цифровизации экономики оказывает значительное влияние и на деятельность страховщиков – хозяйствующих субъектов, осуществляющих страховую деятельность, являющихся основными участниками рынка страхования.

Страховые компании в России достаточно оптимистично оценивают уровень своей цифровизации. Так, уровень цифровизации своей деятельности в 2019 году, более чем в 30% оценивают 37% страховых компаний в России.

Об этом заявил в июне 2019 года руководитель Департамента страхования и экономики социальной сферы Финансового университета при Правительстве РФ

Александр Цыганов на второй всероссийской научно-практической конференции «Первые итоги и драйверы дальнейшего развития цифровизации страхового рынка в Российской Федерации» [1].

Как рассказал со ссылкой на данные исследования Департамента страхования и экономики социальной сферы Финансового Университета при Правительстве РФ Александр Цыганов, практически все страховые компании используют сегодня в своей деятельности технологию "интернетизации бизнес-процессов" (93% респондентов). Половина страховщиков заявляют об использовании технологии больших данных (57%) и новых производственных технологий (47%). Технологией беспроводной связи используются 40% и технологии искусственного интеллекта 30% страховщиков.

Другие новые цифровые технологии, перечисленные в программе Правительства РФ «Цифровая экономика», в том числе технология блокчейн, по словам Александра Цыганова, страховщиками практически не используется.

«Страховщики, принявшие участие в опросе, достаточно оптимистично оценивают уровень цифровизации своей деятельности (отношение бизнес-процессов с использованием новых цифровых технологий к общему числу бизнес-процессов). Так, уровень цифровизации своей деятельности свыше 30% оценивают 37% страховщиков-респондентов. В то же время еще 37% страховщиков полагают, что их уровень цифровизации находится в диапазоне 5-20%», - указал Александр Цыганов.

На высокую оценку уровня цифровизации собственной деятельности, как отметил Александр Цыганов, могли оказать влияние высокая доля интернет-продаж страховых услуг, особенно в сегменте ОСАГО, а также профессиональная принадлежность большинства представителей страховщиков, заполняющих анкеты, к ИТ-подразделениям.

Половина страховых компаний в качестве основных причин низкого уровня развития цифровизации страховой деятельности, по словам Александра Цыганова, указывают высокую стоимость новых цифровых технологий (50%); отсутствие спроса на оцифрованные страховые программы (47%); недостаточную адаптацию цифровых технологий для страховых услуг (47%).

1 июня 2021 года появилась информация о том, что 83% россиян стали чаще пользоваться страховыми онлайн-сервисами на фоне пандемии. Такие данные приводятся по результатам исследования, проведенного Всероссийским союзом страховщиков (ВСС) и AC&M. Цифровыми страховыми услугами за последние 12 месяцев воспользовались 74% респондентов от общего числа потребителей, которые получали страховые услуги за последний год.

Самыми востребованными страховыми онлайн-сервисами стали покупка нового полиса и продление договора страхования (пользовались 51% опрошенных). Следом по

востребованности идут урегулирование онлайн без визита в офис и заявление о страховом случае (29% и 25% опрошенных соответственно).

Результаты потребительского опроса продемонстрировали, что пандемия в совокупности с усилиями страховых компаний стала мощным драйвером цифровизации в сфере онлайн-страхования. Более 60% респондентов осведомлены о цифровых услугах в области страхования (исключение - онлайн-урегулирование, с которым знакомо примерно 50%).

Существенно увеличивается доверие со стороны целевой аудитории к цифровым страховым услугам и готовность целиком перейти на обслуживание онлайн. Все параметры группы Digital Perception (доверие цифровым услугам СК, удовлетворенность от использования цифровых услуг в страховании и готовность перейти на онлайн-обслуживание) выросли по сравнению с первым полугодием 2020 года на 5 п.п.: с 75% до 80%, с 80% до 85% и с 73% до 78% соответственно.

Опрос проводился BCC и AC&M в рамках проекта по вычислению Индекса цифрового застрахованного (ИЦЗ) – первого аналитического показателя в России, оценивающего уровень цифровизации продуктов и услуг страховых компаний для клиентов - физических лиц. Во втором полугодии 2020 г., по сравнению с первым, ИЦЗ вырос на 1 п.п. - с 43% до 44%.

ИЦЗ появился буквально через пару дней после того, как президент России Владимир Путин поручил правительству страны утвердить стратегии цифровой трансформации 10 ключевых отраслей отечественной экономики и социальной сферы.

ИЦЗ рассчитывается на основе трех групп параметров, отражающих взаимодействие страховых компаний с розничными клиентами в цифровой среде: Digital Presence (цифровое присутствие), Digital Practice (цифровая практика) и Digital Perception (цифровое восприятие). Digital Presence оценивает интенсивность взаимодействия страховых компаний и клиентов в цифровых каналах продаж и обслуживания, Digital Practice учитывает возможность онлайн-взаимодействия (причем не только покупки полисов, но и урегулирования страховых случаев), а Digital Perception отражает субъективное восприятие потребителями опыта взаимодействия с цифровыми сервисами (на основе опросов населения).

Как отметила генеральный директор AC&M Марина Белова, тенденция перехода страховых услуг в онлайн сохранится, но темпы этого процесса меняются.

«Не исключаем, что после отмены вынужденной изоляции в первой половине 2021 г. мы будем наблюдать некоторое замедление цифровой трансформации или даже ретроградные процессы. Важно отметить тот факт, что в отрасли есть компании, которые уже продвинулись далеко по пути цифровой трансформации, а есть группа

компаний, которые делают первые шаги, и у них потенциал роста цифровых услуг исчерпан не более чем на 10-15%», – подчеркнула Марина Белова.

Как утверждают специалисты AC&M, судя по двум исследованиям в 2020 г. и 2021 г., доля цифровых услуг постепенно подрастает на 2 п.п. за полугодие. Этот рост, вероятнее всего, будет продолжаться, пока доля онлайн-услуг не достигнет уровня предварительного насыщения. Определенная доля потребителей, может быть 20%, а может быть и 30%, будут пользоваться традиционными витринами и вариантами взаимодействия со страховыми компаниями в обозримой перспективе.

По мнению AC&M, самый большой потенциал у онлайн-урегулирования страховых случаев. Потребитель еще не привык к такой практике и сомневается в ее эффективности. Для того чтобы онлайн-урегулирование стало де-факто стандартом отрасли, пионерам в этой области необходимо обеспечить клиентам яркий положительный пользовательский опыт.

Опрос AC&M показал, что есть некоторые специфические продукты, которые в моменте времени оказались не слишком востребованы. Например, страхование выезда за рубеж (полисы, которые оформлялись почти исключительно онлайн) [2].

Главным препятствием для внедрения любых новых технологий, по мнению респондентов, являются устаревшие и не оптимально организованные собственные ИТ-системы.

Среди специалистов по анализу данных распространено правило GIGO (Garbage in garbage out), согласно которому перед использованием каких-либо моделей необходимо провести тщательную работу с данными. Устаревшие ИТ-системы с разрозненными и противоречащими данными должны быть оптимизированы для успешного внедрения новых технологий.

Крупным игрокам с долгой историей на рынке сложнее реорганизовать имеющиеся ИТ-системы для слаженной работы внедряемых технологий.



Рисунок 1. Препятствия на пути развития новых технологий [3]

С этой точки зрения преимущество могли бы получить небольшие страховщики, готовые инвестировать в иншуртех. Однако, поскольку технологические ИТ-решения остаются дорогостоящими проектами для небольших компаний, шансы игроков на победу в начавшейся «гонке технологий» уравниваются. Кроме того, нельзя игнорировать консерватизм, свойственный страховой отрасли. Для страхователя знакомый много лет крупный страховщик может выглядеть более надежным по сравнению с молодой технологичной компанией [4].

Примечательно, что развитие цифровых финансовых экосистем может привести к возникновению страховых продуктов, выстроенных исключительно на цифровом пути (андеррайтинг на больших данных из экосистем, онлайн-площадки для продаж), и это будет одним из драйверов страхового рынка в ближайшей перспективе.

Согласно анализу, McKinsey&Company, выгода от внедрения новых технологий в страховании на международном рынке может составить 1 100 млрд. долл. США на годовой основе, причем 888 млрд. относятся к технологиям в продажах и маркетинге. Почти четверть страховщиков внедрила роботизацию процессов, хотя 47% опрошенных, после проведения анализа целесообразности в прошлом году, отказались от инвестирования в это направление в ближайшей перспективе. Как и в прошлом году, многие страховщики полноценно используют чат-боты (29%) и облачные технологии (41%) [5].

В качестве вывода следует отметить, что цифровые преобразования изменяют методы, при помощи которых страховщики работают со страхователями. Основное направление таких преобразований – постепенная переориентация деятельности страховщика от «слепого» развития продуктовой линейки к ориентации на потребителя.

Развитие цифровой экономики определяет следующие, востребованные современным рынком направления деятельности страховщиков: клиентоориентированный подход; защита интеллектуальной собственности и результатов интеллектуальной деятельности, создание инновационной культуры.

Библиографический список

1. Тренды развития ИТ в страховании. «Умное» страхование. – Режим доступа: <https://www.tadviser.ru/index.php>
2. Услуги страхования переходят в онлайн. – Режим доступа: <https://www.comnews.ru/content/214750/2021-06-01/2021-w22/uslugi-strakhovaniya-perekhodyat-onlayn>
3. Обзор рынка страхования в России в 2021 году. – Режим доступа: <https://assets.kpmg/content/dam/kpmg/ru/pdf/2021/07/ru-ru-insurance-survey-2021.pdf>
4. Обзор рынка страхования в России в 2020 году. – Режим доступа: <https://assets.kpmg/content/dam/kpmg/ru/pdf/2020/08/ru-ru-insurance-survey-2020.pdf>
5. Artificial intelligence in business. – Режим доступа: <https://www.mckinsey.com/>

Электронное научное издание

ЭКОНОМИЧЕСКИЕ ИССЛЕДОВАНИЯ И РАЗРАБОТКИ

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ЭЛЕКТРОННЫЙ ЖУРНАЛ

№ 9/2021

По вопросам и замечаниям к изданию, а также предложениям к
сотрудничеству обращаться по электронной почте mail@scipro.ru

Подготовлено с авторских оригиналов

ISSN 2542-0208

Формат 60x84/16. Усл. печ. л.4,1. Тираж 100 экз.

Издательство Индивидуальный предприниматель Краснова Наталья Александровна
Адрес редакции: Россия, 603000, г. Нижний Новгород, пл. М. Горького, 4/2, 4 этаж, офис №1