ЭКОНОМИКА И КАЧЕСТВО СИСТЕМ СВЯЗИ ***№ 2(32) / 2024***
Дата выхода: 06.06.2024

ISSN 2500-1833

Международный научно-практический электронный журнал
Основан в 2015 году, издается ежеквартально

Журнал включен в перечень рецензируемых научных изданий, рекомендуемых ВАК Минобрнауки России для публикации научных результатов, отражающих основное научное содержание кандидатских и докторских диссертаций

Учредитель *ООО «Научно-производственное предприятие «Информационные и Радио Технологии»*
Издатель *ООО «Научно-производственное предприятие «Информационные и Радио Технологии»*

Журнал публикует статьи, отражающие результаты исследований в соответствии со следующими разделами ГРНТИ:
06.00.00 – Экономика и экономические науки
20.00.00 – Информатика
28.00.00 – Кибернетика
47.00.00 – Электроника. Радиотехника
49.00.00 – Связь
81.93.29 – Информационная безопасность
82.00.00 – Организация и управление
90.00.00 – Метрология

Адрес редакции: *г. Москва, ул. Малая Тульская, д. 16, эт. 1. пом. I. ком. 20*

сайт: *http://journal-ekss.ru/* ***e-mail:*** *journal-ekss@mail.ru* ***тел.:*** *+7(495)423-57-80*

СОДЕРЖАНИЕ

ЭКОНОМИКА И УПРАВЛЕНИЕ В ИНФОКОММУНИКАЦИЯХ. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ГОСУДАРСТВА И ОБЩЕСТВА. ИНФОКОММУНИКАЦИОННЫЕ БИЗНЕС-ТЕХНОЛОГИИ

СИСТЕМЫ, СЕТИ И УСТРОЙСТВА СВЯЗИ. РАДИОТЕХНИКА. АНТЕННЫ. ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА. ПРИБОРЫ И МЕТОДЫ ИЗМЕРЕНИЯ. МЕТРОЛОГИЯ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ, СЕТИ И ТЕХНОЛОГИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ

ЭКОНОМИКА И УПРАВЛЕНИЕ В ИНФОКОММУНИКАЦИЯХ. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ГОСУДАРСТВА И ОБЩЕСТВА. ИНФОКОММУНИКАЦИОННЫЕ БИЗНЕС-ТЕХНОЛОГИИ

ЧЕЛОВЕЧЕСКИЙ КАПИТАЛ КАК ФАКТОР РАЗВИТИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И СЕТЕВОЙ ЭКОНОМИКИ В СТРАНАХ БЫВШЕГО СССР

К.К. Шебеко, *д.э.н, профессор, Белорусский государственный технологический университет, k.shebeko@tut.by;*
Д.К. Шебеко, *к.э.н., Баер АО, dshabeka@gmail.com.*

УДК 338.001.36

Аннотация. На основе индекса человеческого капитала (*Human Capital Index*) определены прогнозные значения индекса сетевой готовности (*Network Readiness Index)* и валового внутреннего продукта на душу населения по паритету покупательной способности в текущих ценах (международные доллары) (*GDP per capita, PPP* (*current international $*) для стран, входивших в состав СССР. Величина отклонения полученных прогнозных значений индекса сетевой готовности от фактических предложена в качестве показателя, характеризующего эффективность использования располагаемого страной человеческого капитала для развития информационно-коммуникационных технологий и сетевой экономики в актуальном историческом периоде. Установлено, что Молдова, Украина, Армения и Эстония более эффективно используют имеющийся человеческий капитал для развития информационно-коммуникационных технологий и сетевой экономики в исследуемом периоде. Полученные результаты могут быть использованы для обоснования мер и инструментов экономической политики.

Ключевые слова: информационно-коммуникационные технологии; сетевая экономика; индекс сетевой готовности (*Network Readiness Index*); уровень экономического развития; человеческий капитал; постсоветские страны.

HUMAN CAPITAL AS A FACTOR IN THE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES AND NETWORK ECONOMY IN THE POST-SOVIET COUNTRIES

Konstantin Shebeko, *Doctor of Economics, Professor, Belarusian State Technological University;*
Dzmitry Shabeka, *PhD, Bayer AG.*

***Annotation*.** On the basis of the Human Capital Index, the forecast values of the Network Readiness Index and *GDP* per capita, *PPP* (current international dollars) for the countries that were part of the *USSR* are determined. The value of deviation of the determined forecast values of the Network Readiness Index from the actual ones is proposed as an indicator characterising the efficiency of the use of human capital available in the country for the development of information and communication technologies and network economy in the current historical period. It was found that Moldova, Ukraine, Armenia and Estonia use the available human capital for the development of information and communication technologies and network economy

more effectively in the researched period. The obtained results can be used to develop economic policy measures and instruments.

***Keywords*:** information and communication technologies; network economy; Network Readiness Index; level of economic development; human capital; post-Soviet countries.

Введение

Страны, входившие в состав СССР, после его распада в силу различных причин избрали разные модели развития. Прошедший период позволяет сделать некоторые выводы, характеризующие успешность постсоветских государств в реагировании на вызовы, обусловленные процессами, происходящими в мировой экономике, в т.ч. переходом к цифровому обществу.

В исследовательском сообществе сформировался консенсус о ключевой роли человеческого капитала и информационно-коммуникационных технологий в развитии современных обществ. Поэтому исследование различных аспектов влияния человеческого капитала на развитие информационно-коммуникационных технологий и сетевой экономики еще долгое время будут оставаться актуальными. Авторами ставились задачи обоснования прогнозных значений показателей развития стран на основе количественной оценки человеческого капитала и уровня развития информационно-коммуникационных технологий и выявления факторов, которые могли повлиять на эффективность использования человеческого капитала для развития ИКТ в текущем периоде.

Значимость полученных результатов заключается в обосновании величины отклонения полученных прогнозных значений индекса сетевой готовности от фактических в качестве показателя, характеризующего эффективность использования располагаемого страной человеческого капитала для развития информационно-коммуникационных технологий и сетевой экономики в актуальном историческом периоде.

Материалы и методы

В исследовании применены общепринятые формально-логические приемы познания (абстрагирование, анализ и синтез, индукция и дедукция, сравнение и аналогия), приемы и методы эмпирического и конкретно-экономического анализа (описание, измерение), принципы теоретико-экономического исследования (экономический рационализм, «при прочих равных условиях»).

Для изучения факторов, которые могли повлиять на эффективность использования человеческого капитала для развития информационно-коммуникационных технологий и сетевой экономики в текущем периоде, использован методологический подход, известный как «закономерности-тенденции».

Результаты исследования

Описание и доказательства гипотезы о влиянии располагаемого человеческого капитала на развитие общества в целом и экономическую динамику представлены в исследованиях Т. Шульца, Г. Беккера, Р. Солоу, Дж. Кендрика, С. Кузнеца, И. Фишера, Р. Лукаса и других экономистов [1-3].

Статистический анализ экономического развития различных стран в свое время позволил сформулировать гипотезу о влиянии человеческого капитала на уровень развития информационно-коммуникационных технологий и сетевой экономики. Следует отметить, что использование такого подхода, как правило, весьма сложно в силу временных лагов проявления причинно-следственных

связей, недостаточной разработки проблем измерения и доступности релевантной исходной информации [4, 5]. Вместе с тем, для конкретных исторических периодов получить доказательства данной гипотезы вполне возможно [6].

В настоящее время решение проблемы измерения уровня информационно-коммуникационных технологий и сетевой экономики получило дальнейшее развитие благодаря разработке индекса сетевой готовности (*Network Readiness Index*) – комплексного показателя, разработанного в 2002 г. и опубликованного *World Economic Forum* и международной школой бизнеса *INSEAD* в рамках докладов о развитии информационного общества. С 2019 г. индекс публикуется *Portulans Institute* совместно с *World Information Technology and Services Alliance* [7].

Измерение человеческого капитала также потребовало значительных усилий разработчиков [8], в результате которых в 2018 г. был впервые рассчитан индекс человеческого капитала. Наличие этого показателя в значительной мере расширило возможности проведения исследований [9].

Нами изучена взаимосвязь уровня сетевой готовности (измеренного посредством *Network Readiness Index*) и уровня располагаемого человеческого капитала (измеренного посредством *Human Capital Index*) для стран, входивших в состав СССР, с использованием модели, опубликованной ранее [6, с. 18]. Основываясь на принципе «при прочих равных условиях» и методологическом положении «закономерности-тенденции», получены прогнозные значения потенциального индекса сетевой готовности для исследуемых стран (табл. 1).

Таблица 1.

Страны	Индекс человеческого капитала 2020 (*Human Capital Index*)	Индекс сетевой готовности 2022 (*Network Readiness Index*)	Потенциальный индекс сетевой готовности	Отношение фактического индекса сетевой готовности к потенциальному
Азербайджан	0,58	47,74	49,3	0,97
Армения	0,58	50,40	49,3	1,02
Грузия	0,57	47,14	48,2	0,98
Казахстан	0,63	52,46	55,0	0,95
Кыргызстан	0,60	41,03	51,2	0,80
Латвия	0,71	59,86	64,1	0,93
Литва	0,71	62,78	64,1	0,98
Молдова	0,58	49,54	49,3	1,00
Российская Федерация	0,68	59,54	60,6	0,98
Таджикистан	0,50	34,73	40,2	0,81
Украина	0,63	55,71	55,0	1,01
Эстония	0,70	69,79	62,9	1,11

Источник: собственная разработка на основе [7, 9].

Выполнить расчеты по Беларуси, Туркменистану и Узбекистану не удалось в силу отсутствия в открытом доступе необходимой исходной информации.

Данные табл. 1 показывают, что, имеются значительные различия между странами по показателю отклонения полученных прогнозных значений индекса сетевой готовности от фактических. Если рассматривать человеческий капитал как фактор развития информационно-коммуникационных технологий и сетевой экономики, то такое отклонение можно трактовать как показатель эффективности

использования располагаемого страной человеческого капитала в соответствующих целях.

Для обоснования такого подхода рассмотрим результативные показатели развития стран, на которые могла бы повлиять степень использования располагаемого человеческого капитала для развития информационно-коммуникационных технологий и сетевой экономики (табл. 2).

Таблица 2.

Интервал отклонения фактического индекса сетевой готовности от потенциального	Отношение фактического индекса сетевой готовности к потенциальному, в среднем по группе	Рейтинг стран мира по уровню процветания 2023 (*Legatum Institute: Legatum Prosperity Index*)	Уровень социального развития 2015 (*Social Progress Imperative: Social Progress Index*)	Рейтинг стран мира по индексу социального прогресса 2022 (*Social Progress Imperative: Social Progress Index*)	Продолжительность здоровой жизни 2018 (*World Health Organization: Healthy Life Expectancy Index*), лет	Рейтинг стран мира по индексу инноваций 2023 (*INSEAD, WIPO: Global Innovation Index*)
Менее 0,97 Казахстан Кыргызстан Латвия Таджикистан	0,87	59,87	62,64	69,24	64,2	26,2
От 0,97 до 0,99 Российская Федерация Литва Грузия Азербайджан	0,98	62,40	66,54	73,35	64,9	32,1
Более 0,99 Молдова Украина Армения Эстония	1,04	64,13	68,89	77,33	65,5	36,1
Итого, в среднем	0,96	62,13	66,02	73,31	64,9	31,5

Источник: собственная разработка на основе [7, 9-14].

Страны, вошедшие в третью группу (табл. 2), превосходят по степени использования располагаемого человеческого капитала для развития информационно-коммуникационных технологий и сетевой экономики страны второй группы на 6,1%, страны первой группы – на 19,5%. Для них характерно наличие более высокого уровня процветания (*Legatum Institute: Legatum Prosperity Index*) по сравнению со странами, входящими во вторую (на 2,8%) и первую группу (на 7,1%). Соответственно, по уровню социального развития 2015 г. (*Social Progress Imperative: Social Progress Index*) – на 3,5% и на 10,0%; по индексу социального прогресса 2022 г. (*Social Progress Imperative: Social Progress Index*) – на 5,4% и на 11,7%; по индексу инноваций (*INSEAD, WIPO: Global Innovation Index*) – на 12,5% и на 37,8%; по продолжительности здоровой жизни (*World Health Organization: Healthy Life Expectancy Index)* – на 0,9% и на 2,0%.

Таким образом, имеются основания для вывода о возможности рассматривать отклонение полученных прогнозных значений индекса сетевой готовности от фактических как показатель эффективности использования располагаемого страной человеческого капитала.

Рассмотрим факторы институционального характера, которые могли бы

повлиять на степень использования располагаемого человеческого капитала для развития информационно-коммуникационных технологий и сетевой экономики (табл. 3).

Таблица 3.

Интервал отклонения фактического индекса сетевой готовности от потенциального	Индекс качества элит 2023 (*Elite Quality Index*)	Индекс качества элит 2022 (*Elite Quality Index*)	Индекс качества элит 2021 (*Elite Quality Index*)	Изменение доли рентных доходов в ВВП в среднем за 1997-2017 гг., п.п.	Рейтинг стран мира по индексу свободы человека 2022 (*Cato Institute, Fraser Institute: Human Freedom Index*)	Рейтинг стран мира по уровню политических и гражданских свобод 2023 (*Freedom House: Freedom in the World*)	Рейтинг стран мира по индексу качества гражданства 2018 (*Henley & Partners: Quality of Nationality Index*), %
Менее 0,97 Казахстан Кыргызстан Латвия Таджикистан	48,0	48,1	47,1	+4,4	6,77	36	31,3
От 0,97 до 0,99 Российская Федерация Литва Грузия Азербайджан	48,3	50,7	51,9	+2,4	6,94	43	46,7
Более 0,99 Молдова Украина Армения Эстония	51,1	50,7	50,9	+1,6	7,75	65	46,4
Итого, в среднем	49,1	49,8	50,0	+2,8	7,15	48	41,5

Источник: собственная разработка на основе [7, 9, 15-21].

Уровень качества элит (*Elite Quality Index*) в 2023 г. (табл.3) составил в среднем по странам, вошедшим в третью группу, 104,1% по отношению к среднему по исследуемой совокупности, во второй группе – 98,4%, в первой – 97,8%. Соответственно, в 2022 г. – 101,8%, 101,8% и 96,6%, в 2021 г. – 101,8%, 103,8% и 94,2%. Для стран, вошедших в третью группу, характерно наличие более высокого индекса свободы человека (*Cato Institute, Fraser Institute: Human Freedom Index*) по сравнению со странами, входящими во вторую (на 11,7%) и первую группу (на 14,5%). Соответственно, по уровню политических и гражданских свобод (*Freedom House: Freedom in the World* 2023) – на 51,2% и на 80,6%. Следует отметить и превосходство стран, вошедших в третью и вторую группу, по индексу качества гражданства (*Henley & Partners: Quality of Nationality Index* 2018).

Данные табл. 3 показывают, что по мере снижения степени использования располагаемого человеческого капитала для развития информационно-коммуникационных технологий и сетевой экономики можно констатировать увеличение доли рентных доходов в ВВП. Такое положение создает базовые условия для рентоориентированного поведения экономических агентов, что в свою очередь связано с качеством институциональной системы [22].

Результаты изучения параметров качества институциональной системы [23],

которые могли бы повлиять на эффективность использования располагаемого человеческого капитала для развития информационно-коммуникационных технологий и сетевой экономики, представлены в табл. 4.

Таблица 4.

Интервал отклонения фактического индекса сетевой готовности от потенциального	Учет мнения населения и подотчетность государственных органов 2017 (*Voice and Accountability*)	Политическая стабильность и отсутствие насилия 2017 (*Political Stability and Absence of Violence/Terrorism*)	Эффективность работы правительства 2017 (*Government Effectiveness*)	Качество законодательства 2017 (*Regulatory Quality*)	Верховенство закона 2017 (*Rule of Law*)	Сдерживание коррупции 2017 (*Control of Corruption*)
Менее 0,97 Казахстан Кыргызстан Латвия Таджикистан	-0,65	-0,16	-0,23	-0,02	-0,44	-0,67
От 0,97 до 0,99 Российская Федерация Литва Грузия Азербайджан	-0,35	-0,26	+0,33	+0,37	-0,01	-0,12
Более 0,99 Молдова Украина Армения Эстония	+0,16	-0,55	+0,01	+0,39	0,00	-0,23
Итого, в среднем	-0,28	-0,32	0,04	0,25	-0,15	-0,34

Источник: собственная разработка на основе [7, 9, 23].

Анализ данных табл. 4 позволяет констатировать, что для группы стран с более эффективным использованием располагаемого человеческого капитала для развития информационно-коммуникационных технологий и сетевой экономики характерен более высокий уровень качества институциональной системы по следующим параметрам: учет мнения населения и подотчетность государственных органов (*Voice and Accountability*), качество законодательства (*Regulatory Quality*), верховенство закона (*Rule of Law*).

С использованием модели, позволяющей оценить влияние индекса сетевой готовности на экономическое развитие стран [6, с. 15], определены прогнозные значения ВВП на душу населения для исследуемой совокупности стран (табл. 5).

Как видно из данных табл. 5, в наибольшей степени удалось использовать достигнутый уровень информационно-коммуникационных технологий и сетевой экономики для экономического развития в Литве и Казахстане.

Данные для сравнения показателей отдельных стран со средними по исследуемой совокупности представлены в табл. 6.

Таблица 5.

Страны	Индекс сетевой готовности 2022 (*Portulans Institute: Networked Readiness Index*)	Реальный ВВП на душу населения по ППС в 2020 г. (международные доллары в текущих ценах), тыс.	Потенциальный ВВП на душу населения по ППС (международные доллары в текущих ценах), тыс.	Отношение реального ВВП на душу населения по ППС в 2020 г. (международные доллары в текущих ценах) к потенциальному	Возможный ВВП на душу населения по ППС по потенциальному индексу сетевой готовности (международные доллары в текущих ценах), тыс.
Азербайджан	47,74	14,5	22,2	0,65	24,1
Армения	50,40	13,3	25,3	0,53	24,1
Грузия	47,14	14,8	21,5	0,69	22,8
Казахстан	52,46	26,7	27,8	0,96	30,7
Кыргызстан	41,03	5,0	14,4	0,35	26,3
Латвия	59,86	32,2	36,4	0,88	41,4
Литва	62,78	39,2	39,8	0,98	41,4
Молдова	49,54	13,0	24,2	0,54	24,1
Российская Федерация	59,54	28,2	36,0	0,78	37,3
Таджикистан	34,73	3,9	7,0	0,56	13,4
Украина	55,71	13,1	31,6	0,41	30,7
Эстония	69,79	37,9	48,0	0,79	40,0

Источник: собственная разработка на основе [7, 9, 18].

Таблица 6.

Страны	Индекс человеческого капитала, 2020 (*Human Capital Index*), в процентах к среднему по совокупности	Индекс сетевой готовности 2022 (*Portulans Institute: Networked Readiness Index*), в процентах к среднему по совокупности	Реальный ВВП на душу населения по ППС в 2020 г. (международные доллары в текущих ценах), в процентах к среднему по совокупности	Потенциальный ВВП на душу населения по ППС (международные доллары в текущих ценах), в процентах к среднему по совокупности	Возможный ВВП на душу населения по ППС по потенциальному индексу сетевой готовности (международные доллары в текущих ценах), в процентах к среднему по совокупности
Азербайджан	93,5	90,8	71,8	79,6	81,1
Армения	93,5	95,9	65,8	90,7	81,1
Грузия	91,9	89,7	73,3	77,1	76,8
Казахстан	101,6	99,8	132,2	99,6	103,4
Кыргызстан	96,8	78,1	24,8	51,6	88,6
Латвия	114,5	113,9	159,4	130,5	139,4
Литва	114,5	119,4	194,1	142,7	139,4
Молдова	93,5	94,3	64,4	86,7	81,1
Российская Федерация	109,7	113,3	139,6	129,0	125,6
Таджикистан	80,6	66,1	19,3	25,1	45,1
Украина	101,6	106,0	64,9	113,3	103,4
Эстония	112,9	132,8	187,6	172,0	134,7

Источник: собственная разработка на основе [7, 9, 18].

На основе данных табл. 6 можно сделать вывод о более высоких возможностях экономического развития за счет фактора информационно-коммуникационных технологий и сетевой экономики у следующих стран: Эстония, Литва, Латвия, Российская Федерация, Украина, Казахстан.

Заключение

Таким образом, на основе предлагаемого показателя величины отклонения прогнозных значений индекса сетевой готовности от фактических, можно сделать вывод, что Молдова, Украина, Армения и Эстония более эффективно используют имеющийся человеческий капитал для развития информационно-коммуникационных технологий и сетевой экономики в исследуемом периоде.

Вместе с тем, оценивая возможный ВВП на душу населения по ППС (международные доллары в текущих ценах) на основе прогнозного индекса сетевой готовности (получен на основе располагаемого каждой страной человеческого капитала), следует отметить, что Латвия, Литва, Эстония, Российская Федерация, Казахстан и Украина превосходят среднее значение по исследуемой группе стран, а Таджикистан, Грузия, Азербайджан, Армения, Молдова и Кыргызстан имеют этот показатель ниже среднегруппового значения.

Литература

1. Зоткина Н.С., Гусарова М.С., Копытова А.В. Человеческий капитал как ведущий фактор развития компании: монография. – Чебоксары: Издательский дом «Среда», 2021. – 164 с.
2. Кендрик Дж. Совокупный капитал США и его функционирование. – М.: Прогресс, 1976.
3. Шебеко К.К., Грошев В.А., Шебеко Д.К. Человеческий капитал и экономическое развитие: Беларусь и соседние страны // Экономическая наука сегодня, 2022. – № 16. URL: https://cyberleninka.ru/article/n/chelovecheskiy-kapital-i-ekonomicheskoe-razvitie-belarus-i-sosednie-strany (дата обращения: 19.03.2024).
4. James J. Sharing Mechanisms for Information Technology in Developing Countries, Social Capital and Quality of Life. Social Indicators Research, 2009. – №. 94 (1). – pp. 43-59.
5. Ellis L.A., Collin P., Davenport T.A., Hurley P.J., Burns J.M., Hickie I.B. Young men, mental health, and technology: Implications for service design and delivery in the digital age. J. Med. Internet Res, 2012. – № 14 (6). – pp. 417-430.
6. Шебеко К.К., Шебеко Д.К. Развитие информационно-коммуникационных технологий и сетевой экономики в Беларуси и соседних странах // Экономика и качество систем связи, 2023. – №1 (27). URL: https://cyberleninka.ru/article/n/razvitie-informatsionno-kommunikatsionnyh-tehnologiy-i-setevoy-ekonomiki-v-belarusi-i-sosednih-stranah (дата обращения: 19.03.2024).
7. Рейтинг стран мира по Индексу сетевой готовности / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006–2023 (последняя редакция: 14.10.2023). URL: https://gtmarket.ru/ratings/networked-readiness-index (дата обращения 23.02.2024).
8. Mulligan C.B. X.Sala-i-Martin. Measuring Aggregate Human Capital. — Working Paper of the NBER, No 5016 (Feb. 1995).
9. World Bank Human Capital Project // The World Bank Data URL: https://www.worldbank.org/en/publication/human-capital#Index/ (дата обращения: 09.01.2022).
10. Рейтинг стран мира по уровню процветания / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006–

2023 (последняя редакция: 17.10.2023). URL: https://gtmarket.ru/ratings/legatum-prosperity-index (дата обращения 23.02.2024).
11. Social Progress Imperative: Рейтинг стран мира по уровню социального прогресса 2015 года. [Электронный ресурс] // Центр гуманитарных технологий. — 10.04.2015. 08:00. URL: https://gtmarket.ru/news/2015/04/10/7126 (дата обращения 13.03.2024).
12. Рейтинг стран мира по уровню социального развития / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006-2023(последняя редакция: 20.10.2023).
URL: https://gtmarket.ru/ratings/social-progress-index (дата обращения 13.03.2024).
13. Рейтинг стран мира по уровню продолжительности здоровой жизни / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006-2023 (последняя редакция: 14.10.2023).
URL: https://gtmarket.ru/ratings/healthy-life-expectancy-index (дата обращения 13.03.2024).
14. Рейтинг стран мира по Индексу инноваций / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006–2023 (последняя редакция: 14.10.2023). URL: https://gtmarket.ru/ratings/global-innovation-index (дата обращения 23.02.2024).
15. Рейтинг стран мира по индексу качества элит / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006–2023 (последняя редакция: 14.10.2023). URL: https://gtmarket.ru/ratings/elite-quality-index(дата доступа 20.11.23).
16. Casas, Tomas and Cozzi, Guido, Elite Quality Report 2023: Country Scores and Global Rankings (April 25, 2023). Zurich: Seismo. 2023, https://doi.org/10.33058/seismo.30882.0001, Available at SSRN: https://ssrn.com/abstract=4418550 (дата обращения 23.02.2024).
17. Casas, Tomas and Cozzi, Guido, Elite Quality Report 2022: Country Scores and Global Rankings (April 28, 2022). Zurich: Seismo. 2022 doi: 10.33058/ seismo.30769.0001, Available at SSRN: https://ssrn.com/abstract=4085752 (дата обращения 23.02.2024).
18. World Bank Open Data // The World Bank Data URL: https://data.worldbank.org/ (data obrashcheniya: 02.04.2021).
19. Рейтинг стран мира по Индексу свободы человека / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006-2023 (последняя редакция: 29.10.2023).
URL: https://gtmarket.ru/ratings/human-freedom-index (дата обращения 13.03.2024).
20. Рейтинг стран мира по уровню политических и гражданских свобод / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006-2023 (последняя редакция: 29.10.2023). URL: https://gtmarket.ru/ratings/freedom-in-the-world (дата обращения 13.03.2024).
21. Рейтинг стран мира по Индексу качества гражданства / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006–2023(последняя редакция: 14.10.2023).
URL: https://gtmarket.ru/ratings/henley-nationality-index (дата обращения 13.03.2024).
22. Шебеко К.К., Грошев В.А., Шебеко Д.К. Рента, качество институтов и экономическое развитие // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук, 2021. – № 1. URL: https://cyberleninka.ru/article/n/renta-kachestvo-institutov-i-ekonomicheskoe-razvitie

(дата обращения: 20.03.2024).
23. The Worldwide Governance Indicators (WGI) project [Электронный ресурс] // Worldwide Governance Indicators – Режим доступа: https://info.worldbank.org/governance/wgi/ (дата обращения: 02.04.2024).

ПОДХОДЫ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ПЛАТФОРМЕННЫХ СЕРВИСОВ

О.И. Шаравова, *к.э.н., доцент, Московский технический университет связи и информатики, o.i.sharavova@mtuci.ru;*
П.А. Жолтикова, *Московский технический университет связи и информатики, polina.zholtikova@gmail.com.*

УДК 33+65 (075.8)

Аннотация. В статье обосновываются методические положения по оценке эффективности применения платформенных сервисов для построения и совершенствования бизнес-процессов в цифровой среде, учитывающие потребности малых и средних предпринимателей с соблюдением требований кибербезопасности. Представлены разработанные методические принципы комплексной оценки процесса цифровизации, соответствующие стратегической карте цифровой трансформации.

Ключевые слова: платформенные сервисы; цифровизация; бизнес-процесс; цифровая экономика; инфокоммуникационные технологии.

EVALUATING THE EFFECTIVENESS OF USING PLATFORM SERVICES

O.I. Sharavova, *Ph. D. in Economics, associate Professor, Moscow Technical University of Communications and Informatics;*
P.A. Zholtikova, *Moscow Technical University of Communications and Informatics.*

Annotation. The article substantiates methodological provisions for evaluating the effectiveness of using platform services to build and improve business processes in a digital environment, taking into account the needs of small and medium-sized entrepreneurs in compliance with cybersecurity requirements. The developed methodological principles of a comprehensive assessment of the digitalization process, corresponding to the strategic map of digital transformation, are presented.

Keywords: platform services; digitalization; business process; digital economy; information and communication technologies.

Введение

Цифровая трансформация становится важнейшим условием успешного функционирования предприятий, развития экономики и улучшения социальной сферы [1-3]. Этот процесс подразумевает не просто внедрение отдельных цифровых технологий, а комплексное преобразование всех видов деятельности организации, и затрагивает множество уровней производства и потребления, начиная от управления ресурсами и заканчивая разработкой новых продуктов и услуг [4-6]. Он также включает в себя использование интернета вещей, искусственного интеллекта и виртуальной реальности для оптимизации производственных процессов, управления операциями и повышения

эффективности маркетинга [7-9]. Кроме того, цифровая трансформация предполагает повышение цифровых компетенций сотрудников для того, чтобы они могли успешно адаптироваться к новым условиям работы и использовать все возможности, предоставляемые цифровыми технологиями [10]. Это помогает предприятиям расти и развиваться, а также улучшает качество жизни людей в целом.

В современном мире наблюдается заметный рост популярности платформенных и кроссплатформенных решений, предназначенных для малых и средних предприятий (МСП) [11-15]. Такая тенденция обусловлена привлекательностью комплексного подхода, который позволяет организовать бизнес-процессы и решить целый спектр операционных и стратегических задач на нескольких иерархических уровнях.

В статье представлены разработанные методические положения по оценке эффективности применения платформенных сервисов для построения и совершенствования бизнес-процессов в цифровой среде, учитывающие потребности предпринимателей с соблюдением требований кибербезопасности, которые позволят оценить эффект от применения платформенных сервисов и возможности совершенствования бизнес-процессов.

Технологии цифровой трансформации в сфере бизнеса

Характерной особенностью цифровой трансформации является ее динамичный характер, когда основополагающие технологии и бизнес-модели постоянно претерпевают эволюционные изменения, зависящие от особенностей деятельности, демографии, экономической динамики и других концептуальных предпосылок [16-20]. В настоящее время можно выделить целый ряд инструментов, технологий и приложений, которые тесно переплетаются с цифровой трансформацией в сфере бизнеса:

1. Аналитические платформы и приложения, основанные на технологии *BigData*, служат важнейшими инструментами для сбора, обработки данных и получения аналитических выводов из огромных массивов данных.

2. Мобильные инструменты и приложения повсеместно присутствуют в сфере цифровой трансформации. Данные технологии способствуют расширению возможностей подключения, доступности и функциональности, легко отвечая потребностям все более мобильно-ориентированной бизнес-среды.

3. Платформы для создания государственных услуг, примером которых являются облачные решения, представляют собой еще один неотъемлемый компонент. Они обеспечивают повышенную эффективность, масштабируемость и доступность, тем самым поддерживая архитектуру государственных услуг.

4. Инструменты и приложения социальных сетей, с которыми неразрывно связана социальная сторона цифровой трансформации. Такие инструменты не только служат каналами коммуникации и вовлечения, но и играют ключевую роль в формировании повествования о бренде и взаимодействии с потребителями.

5. Интернет вещей (*IoT*), «умные» сети и технологии «умного» дома являются квинтэссенцией современного технологического подхода в рамках цифровой трансформации. Эти взаимосвязанные системы обеспечивают бесперебойную связь, автоматизацию и интеллект, способствуя развитию сетевой экосистемы.

Цифровые технологии оказывают глубокое и преобразующее влияние на организации и отрасли, порождая новые цифровые бизнес-модели. Стратегическое исследование требует комплексного подхода к применению структурных составляющих в производственной цепочке создания стоимости, охватывающей

как основной, так и прочие виды деятельности компаний. Следовательно, стратегическая карта включает в себя критические структурные компоненты, такие как финансы, клиенты, процессы, персонал и технологии, как показано на рис. 1, согласование которых является стратегическим принципом для повышения устойчивости, конкурентоспособности и эффективности организации в цифровой среде [21].

Эта модель стратегического картирования крайне важна для навигации по сложному ландшафту цифровой трансформации, поскольку она формирует всеобъемлющую схему, включающую основные области, имеющие ключевое значение для эволюции организации. Трансформация мира цифровых технологий затрагивает все звенья организации. Увеличение производительности компании напрямую зависит от тонкостей улучшения каждого компонента стратегического плана. Целостный подход, при котором каждый стратегический элемент подвергается доработке, имеет первостепенное значение для обеспечения повышения эффективности бизнеса в современных условиях.

Рисунок 1

Инновационная стратегия инвестирования позволяет цифровой трансформации не только сократить издержки, но и обеспечить финансовую устойчивость, открывая новые возможности для увеличения доходов и повышения рентабельности. Бизнес в сфере информационно-коммуникационных технологий часто характеризуется напрямую прямым взаимодействием между производителем и потребителем. Современным информационно-коммуникационным компаниям, действующим в цифровой среде и умело применяющим современные технологии для анализа массивов данных и прогнозирования рыночных тенденций, необходимо тщательно изучать потребительское поведение и эффективно управлять каналами взаимодействия.

Методические положения по оценке эффективности применения платформенных сервисов

Разработка стратегии цифровизации для малых и средних предприятий (МСП) требует применения структурированной методологии, состоящей из нескольких этапов, которые последовательно выполняются для обеспечения комплексного и эффективного процесса цифровой трансформации (рис. 2):

1. ***Анализ уровня цифровизации.*** Начальный этап включает в себя глубокий анализ технологической инфраструктуры, организационных рабочих процессов и существующих цифровых компетенций. Этот критический анализ служит основополагающим шагом к определению базовой линии для последующих стратегических мероприятий.

2. ***Формулировка цели.*** После проведения комплексной оценки внимание переключается на создание образа желаемого цифрового будущего МСП. Этот этап включает в себя создание концепции идеализированного цифрового состояния, согласованного с основными целями и устремлениями бизнеса. Она служит основой для последующих стратегических решений в области цифровизации и начинаний.

3. ***Формирование рабочей команды.*** На этом этапе особое внимание уделяется формированию и согласованию команды, обладающей необходимым набором навыков для реализации намеченной стратегии цифровизации. Динамизм команды, ее опыт, высокий профессиональный уровень и разносторонность подготовки становятся ключевыми факторами, способствующими созданию благоприятной среды для успешной реализации.

4. ***Разработка системы показателей цифровизации.*** Неотъемлемой частью стратегии цифровизации является разработка надежной системы цифровых показателей, которые послужат количественными метриками для оценки прогресса и эффективности инициативы по цифровой трансформации.

5. ***Анализ рисков –*** этап проведения комплексной оценки потенциальных рисков и проблем, которые могут помешать беспрепятственному осуществлению стратегии цифровизации. Разрабатываются стратегии снижения рисков для упреждающего решения непредвиденных ситуаций и повышения устойчивости системы цифровизации.

6. ***Формирование стратегии цифровизации.*** Этап включает в себя определение ключевых приоритетов, распределение ресурсов и разработку последовательного плана действий по воплощению концепции в реальные результаты и осуществляется на основе полученных на предыдущих этапах аналитических данных.

7. ***Оценка готовности к изменениям.*** Признавая неразрывную связь между цифровой трансформацией и организационной культурой, этот этап подчеркивает необходимость согласования корпоративной этики с принципами стратегии цифровизации. Формирование корпоративных ценностей, способствующих развитию инноваций, адаптации и постоянному совершенствованию, способствует успеху инициативы преобразований.

8. ***Дорожная карта.*** Данный этап подразумевает синтез всех предыдущих элементов в комплексную дорожную карту. Дорожная карта определяет структурированную хронологию мероприятий, этапы и контрольные показатели для поэтапной реализации стратегии цифровизации, обеспечивая систематическое и взвешенное продвижение к запланированному цифровому состоянию.

Рисунок 2

Цифровые стратегии, несмотря на различия в их конкретном применении, имеют общие основополагающие принципы, которые делают их аналогичными. Следовательно, необходимо подчеркнуть универсальность ключевых соображений, которые требуют постоянного внимания и изучения.

Прежде чем приступать к разработке цифровой стратегии, необходимо убедиться в том, что в организации существует хорошо отлаженная система управления. Построение надежной системы управления процессами подразумевает создание структурированной последовательности воспроизводимых шагов, обеспечивающей четкость и последовательность выполнения задач любой группой исполнителей процесса. Это способствует беспрепятственному вхождению в процесс отдельных сотрудников, поскольку они имеют четкое представление о своих ролях и обязанностях.

Одновременно с этим необходимо изучить, как организация контролирует как процессную, так и проектную деятельность. Процессы, характеризующиеся регулярным и повторяющимся характером, контрастируют с проектами, которые представляют собой особые начинания, направленные на объединение результатов различных процессов и различных рабочих групп, участвующих в межфункциональном или межведомственном сотрудничестве. Слияние усовершенствованных процессов, проектов и управления закладывает основу для плавного перехода к управлению изменениями. Эта фаза включает в себя повышение уровня вовлеченности, повышение осведомленности.

Показатели эффективности применения платформенных сервисов

Оценку эффективности применения платформенных сервисов предлагается осуществлять поэтапно и в комплексе (рис. 3) на основе определения и анализа следующих характеристик:

1) показателей эффективности работы с клиентами;
2) операционно-процессных показателей;
3) показателей эффективности работы персонала;
4) показателей синергетической эффективности деятельности.

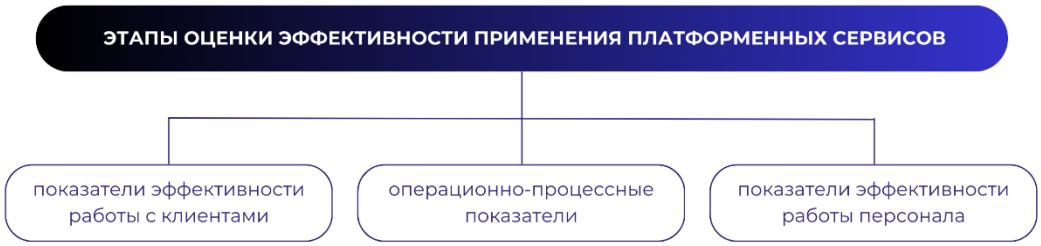

Рисунок 3

Оценка результатов эффективности работы с клиентами выходит за рамки общих маркетинговых показателей и включает в себя специализированные метрики, зависящие от конкретных маркетинговых инструментов, и включает в себя:

- Повышение эффективности продвижения, означающее влияние цифровой трансформации на охват и резонанс маркетинговых кампаний.
- Увеличение коэффициента конверсии, означающее эффективность цифровых инициатив в преобразовании потенциальных клиентов в реальных покупателей.
- Увеличение числа потребителей и расширение охвата целевой аудитории – важные показатели, отражающие рост влияния стратегий цифровой трансформации.
- Расширение точек контакта, что дает больше возможностей для взаимодействия между клиентами и компанией, укрепляя их вовлеченность.
- Большее участие клиентов в цифровых маркетинговых инициативах и коммуникационных каналах свидетельствует об эффективности цифровых стратегий и активном вовлечении.
- Уменьшение времени на запуск новых продуктов на рынок – явный показатель гибкости, которую приносит цифровая трансформация в процессы выведения продукции на рынок.
- Увеличение пожизненной стоимости клиента, которая показывает устойчивое и долгосрочное влияние цифровых инициатив на отношения с клиентами и их лояльность.

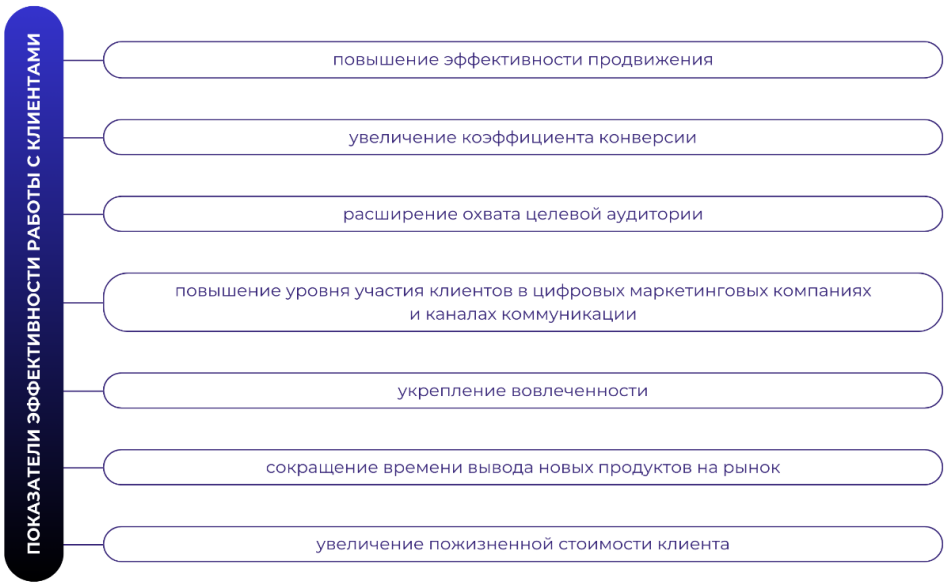

Рисунок 4

Показатели эффективности работы с клиентами (рис. 4) демонстрируют вариативность системы оценивания, обеспечивая целостное понимание меняющейся динамики эффективности маркетинга и вовлечения клиентов.

Операционно-процессные показатели (рис. 5) послужат инструментальными ориентирами для оценки качественных аспектов влияния цифровой трансформации на тонкости бизнес-процессов и включают в себя:

- количественный показатель, отражающий сокращение времени выполнения процессов благодаря цифровой трансформации, что подтверждает повышение эффективности;
- ключевой нефинансовый показатель, связанный с улучшением точности операций, означающий высокую степень точности при использовании цифровых технологий в операционной системе;
- уменьшение количества ошибок за счет уменьшения человеческого вмешательства – важный показатель цифровой трансформации, освидетельствующий обеспечение безупречности бизнес-процессов благодаря автоматизации и технологическим инновациям.

Рисунок 5

Акцент на операционно-процессных показателях эффективности, точности и сокращении ошибок подчеркивает трансформационный потенциал цифровых инициатив в оптимизации основных рабочих процессов предприятия.

На уровне работы персонала выделяются следующие показатели оценки эффективности (рис. 6):

- повышение производительности труда, обозначающее рост эффективности, достигнутый благодаря инициативам цифровой трансформации на уровне отдельных сотрудников;
- повышение компетентности и опыта сотрудников, означающий развивающее воздействие цифровых инициатив на набор навыков и базу знаний рабочей силы;
- сокращение времени рутинной работы за счет автоматизации процессов, подчеркивающее рационализацию операционных рабочих процессов и смягчение рутинных задач за счет технологического вмешательства;
- наличие аналитики для сотрудников, акцентирующее, что данные, полученные с помощью цифровых инструментов, способствуют принятию обоснованных решений, касающихся управления персоналом.

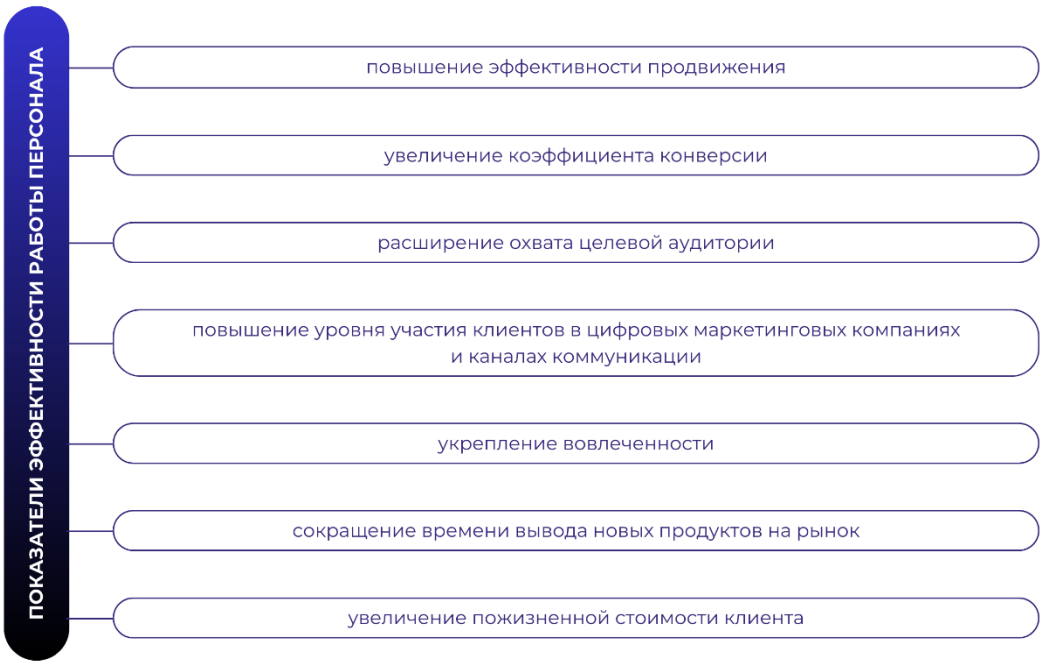

Рисунок 6

Показатели эффективности применения платформенных сервисов на уровне персонала отражают многогранное воздействие цифровой трансформации на динамику развития отдельных сотрудников, раскрывая такие аспекты трансформации, как повышение производительности, развитие навыков, эффективность процессов и поддержка принятия решений на основе данных в рамках организации.

Для комплексной оценки процесса цифровизации предлагаются следующие показатели с определенными временными интервалами:

- контроль и управление данными из единой системы;
- защита от цифровых угроз;
- обучение персонала перед переходом к цифровизации.

Показатели синергетической эффективности [19, 20] деятельности позволяют всесторонне оценить эффективность применения платформенных сервисов, учитывая множество её проявлений, и количественно измерить эту эффективность как в текущий момент времени, так и в перспективе. Это помогает ранжировать цифровые сервисы по интегральному коэффициенту эффективности и обоснованно выбирать наиболее эффективные из них.

Синергетическая эффективность различных платформенных сервисов обладает индивидуальными характеристиками, которые могут значительно отличаться в зависимости от типа и функционала этих сервисов. Универсальная методика расчёта и группировки частных показателей учитывает положительные (результативные) и отрицательные (затратные) аспекты экономической и социальной эффективности.

Однако важной методической задачей является разработка индивидуального перечня частных показателей синергетической эффективности для каждого конкретного платформенного сервиса. На рис. 7 в качестве примера приведена иерархия системы частных показателей синергии эффективности цифрового платформенного сервиса.

Для оценки процесса перехода компании к цифровой трансформации предложено рассмотрение шести траекторий с установленными временными интервалами:

1. Анализ стратегии управления данными, методов их сбора, способов хранения и систем анализа данных, направленных на повышение эффективности принятия решений на основе информации.

2. Интеграция предприятия и производственного оборудования в общую сеть для расширения возможностей подключения.

3. Внедрение цифровых технологий проектирования, моделирования и персонализации продукции, а также использование роботизированных технологий для увеличения гибкости производственных процессов.

4. Интеграция данных предприятия и участников цепочки поставок для оптимизации обмена информацией и ресурсами.

5. Разработка и внедрение надежных стратегий кибербезопасности для защиты организационной инфраструктуры от внешних угроз в цифровом мире.

6. Предоставление рекомендаций и инициатив по обучению сотрудников для обогащения их знаний и навыков с целью акцентировать внимание на человеческом факторе цифровой трансформации.

Таким образом, в свете этих подходов к измерению последствий цифровой трансформации необходимо подходить через оценку технических и экономических показателей, заложенных в бизнес-процессах, человеческих и технологических ресурсах. Эта многомерная система позволяет провести целостную оценку сложных аспектов цифровой трансформации.

Рисунок 7

Заключение

Переход от создания надежной системы управления к совершенствованию процессов, проектов и управления завершается сложным процессом управления изменениями. Этот многогранный подход включает в себя преодоление сопротивления, повышение уровня вовлеченности, повышение осведомленности и формирование у заинтересованных сторон желания активно участвовать в реализации широких преобразовательных инициатив. Систематическая организация этих последовательных этапов подчеркивает всеобъемлющий характер эволюции организации в сторону цифровизации бизнеса и устойчивости.

Разработанные методические положения обеспечивают надежный и системный подход к разработке и реализации стратегии цифровизации с учетом уникальной динамики МСП. Каждый этап и компонент вносит синергетический вклад в достижение общей цели − формирование устойчивой организационной парадигмы, ориентированной на цифровые технологии.

Сформулированные методические принципы разработки стратегии цифровизации предприятий на основе применения цифровых сервисов позволят более точно контролировать все этапы бизнес-процесса и укрепить позиции инфокоммуникационной компании на рынке, свидетельствуя о стремлении содействовать цифровой трансформации бизнеса с помощью инновационных и целевых решений.

Литература

1. Кузовкова Т.А., Шаравова О.И. Цифровая трансформация экономики: учебное пособие. – М.: Ай Пи Ар Медиа, 2023. – 140 с.

2. Кузовкова Т.А., Шаравова О.И., Шаравова М.М. Эволюция перехода к парадигме гармоничного развития и экономической сбалансированной модели гармоничного общества // РИСК: Ресурсы, Информация, Снабжение, Конкуренция, 2022. – № 4. – С. 56-68.

3. Кузовкова Т.А., Кузовков Д.В., Шаравова О.И. Задачи и требования цифровой экономики к развитию инфокоммуникаций // Экономика и качество систем связи, 2019. – № 4 (14). – С. 20-28.

4. Кузовкова Т.А., Шаравова О.И. Основы цифровой экономики: учебное пособие для бакалавров. – Москва: Ай Пи Ар Медиа, 2022. – 128 с.

5. Кузовкова Т.А., Девяткин Е.Е., Тихвинский В.О., Шаравова О.И. Перспективы развития цифровых услуг интеллектуального мира на основе сетей подвижной связи новых поколений // РИСК: Ресурсы, Информация, Снабжение, Конкуренция, 2022. – № 2. – С. 80-86.

6. Кузовкова Т.А., Девяткин Е.Е., Тихвинский В.О., Шаравова О.И. Сети мобильной связи новых поколений – ключевой фактор развития инновационных продуктов интеллектуального мира // РИСК: Ресурсы, Информация, Снабжение, Конкуренция, 2023. – № 2. – С. 151-163.

7. Абдурахманов К.Х. Искусственный интеллект – основа устойчивого развития экономики. –М.: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2023. – 356 с.

8. Кузовкова Т.А., Алмаева О.П., Вольнов А.А., Шаравов И.М. Реализация сценариев использования технологий на базе сетей пятого поколения // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 48-й Международной конференции. Москва, 2021. – С. 30-33.

9. Кузовкова Т.А., Жолтикова В.Р., Жолтикова П.А., Шаравова М.М. Тенденции развития мобильного маркетинга в России // Мобильный бизнес: перспективы

развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 46-й Международной конференции. Москва, 2020. – С. 36-39.
10. Кузовкова Т.А., Ваховский Е.В., Салютина Т.Ю., Шаравова О.И. Влияние цифровой трансформации общества на эволюцию профессиональных и личностных качеств специалистов экономики и управления // РИСК: Ресурсы, Информация, Снабжение, Конкуренция, 2023. – № 4. – С. 166-174.
11. Жолтикова П.А., Ермолаева В.Р. Цифровизация малого и среднего предпринимательства // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: сборник материалов (тезисов) L международной конференции, Москва, 26-27 октября 2022 года. – Москва: Национальный институт радио и инфокоммуникационных технологий, 2022. – С. 55-58.
12. Шаравова О.И., Жолтикова П.А., Ермолаева В.Р. Цифровая трансформация малого и среднего предпринимательства на основе платформенных сервисов // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 52-й Международной конференции. Москва, 2023. – С. 98-101.
13. Шаравова О.И., Жолтикова В.Р., Жолтикова П.А. Использование цифрового сервиса «МЕГАФОН. ТАРГЕТ» для продвижения бизнеса // Экономика и качество систем связи, 2022. – № 2 (24). – С. 9-15.
14. Шаравова О.И., Гумерова Э.М. Значение инструментов и каналов цифрового маркетинга для повышения эффективности экономической деятельности предприятий общественного питания // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 52-й Международной конференции. Москва, 2023. – С. 143-145.
15. Шаравова О.И., Жолтикова П.А., Ермолаева В.Р. Возможности и преимущества цифровых решений для бизнеса // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 51-й Международной конференции, Москва, 24-26 апреля 2023 года. – Москва: ЗАО «Национальный институт радио и инфокоммуникационных технологий», 2023. – С. 86-89.
16. Кузовкова Т.А., Шаравова О.И., Шаравова М.М. Интегральный платформенный характер бизнес-моделей цифровых компаний // РИСК: Ресурсы, Информация, Снабжение, Конкуренция, 2021. – № 2. – С. 107-113.
17. Шаравова М.М. Выявление характера цифровой трансформации моделей инфокоммуникационного бизнеса // Экономика и качество систем связи, 2021. – № 1 (19). – С. 3-12.
18. Кузовкова Т.А., Салютина Т.Ю., Шаравова О.И. Введение в экономику цифровых платформ: учебное пособие. – М.: Ай Пи Ар Медиа, 2022. – 129 с.
19. Кузовкова Т.А., Шаравова О.И., Кузовков А.Д., Шаравова М.М. Значение платформенного бизнеса и методические основы измерения синергии эффективности цифровых платформ // РИСК: Ресурсы, Информация, Снабжение, Конкуренция, 2022. – № 1. – С. 82-91.
20. Кузовкова Т.А., Кузовков А.Д., Шаравов И.М. Понятие ценности цифровых платформ и методы оценки синергии их эффективности // Электронный научный журнал «Век качества», 2022. – № 3. – С.73-96.
21. Кузовкова Т.А., Шаравова М.М., Алмаева О.П. Конвергентный характер стратегии цифровой трансформации инфокоммуникационной компании // Экономика и качество систем связи, 2021. – № 3 (21). – С. 3-19.

АНАЛИЗ И РАЗВИТИЕ ПОДХОДОВ К ФОРМИРОВАНИЮ СТРАТЕГИИ РЕАЛИЗАЦИИ ЦИФРОВЫХ ПРОДУКТОВ И СЕРВИСОВ

Т.А. Кузовкова, *д.э.н., профессор, Московский технический университет связи и информатики, t.a.kuzovkova@mtuci.ru;*
В.Р. Ермолаева, *Московский технический университет связи и информатики, v.r.ermolaeva@mtuci.ru.*

УДК 33+65 (075.8)

Аннотация. В статье раскрыта сущность бизнес-моделей на примере компаний инфокоммуникационной отрасли. Исследованы международные и российские решения по формированию стратегии цифрового продукта или сервиса. На основе анализа теоретических и практических результатов предложены методические подходы по формированию стратегии реализации цифровых продуктов и сервисов в условиях их развития в ходе цифровой трансформации экономики.

Ключевые слова: бизнес-модель; цифровая экономика; стратегия развития; продуктовая стратегия; цифровой продукт; цифровой сервис; подходы к формированию стратегии; инфокоммуникации.

ANALYSIS AND DEVELOPMENT OF APPROACHES TO THE FORMATION OF A STRATEGY FOR THE IMPLEMENTATION OF DIGITAL PRODUCTS AND SERVICES

T.A. Kuzovkova*, Doctor of Economics, Professor, Moscow Technical University of Communications and Informatics;*
V.R. Ermolaeva, *Moscow Technical University of Communications and Informatics.*

Annotation. The article reveals the essence of business models using the example of companies in the infocommunication industry. International and Russian solutions for the formation of a digital product or service strategy are investigated. Based on the analysis of theoretical and practical results, methodological approaches are proposed for the formation of a strategy for the implementation of digital products and services in the context of their development during the digital transformation of the economy.

Keywords: business model; digital economy; development strategy; product strategy; digital product; digital service; approaches to strategy formation; infocommunications.

Введение

Интеграция цифровых технологий во все экономические сферы – от промышленности, сельского хозяйства и транспорта до строительства, здравоохранения и образования – привела к значительным изменениям в бизнес-моделях организаций. Одним из ключевых элементов бизнес-модели любой организации является ценностное предложение – продукты или услуги, которые создаются для удовлетворения нужд потребителей.

Благодаря появлению цифровых и инфокоммуникационных технологий ценностным предложением становятся новые категории – цифровые продукты и сервисы, имеющие существенные особенности с точки зрения содержания и способов реализации. Эффективное развитие цифровых продуктов и сервисов проводится в соответствии с продуктовой стратегией, которая в свою очередь

является частью стратегии развития предприятия и общей бизнес-модели организации [1-4].

В статье представлены результаты анализа и развития подходов по формированию стратегии развития цифрового продукта или сервиса.

Сущность бизнес-моделей на примере оператора подвижной связи

Употребление термина бизнес-модели в максимально близком к современному значению началось практически одновременно с зарождением концепции цифровой экономики и связано со стремлением представить различие между традиционными бизнесами и интернет-компаниями. С помощью бизнес-моделей пытались описать деятельность технологических компаний, формализовать базовые составляющие стартапов в цифровой экономике, для трассировки успешного опыта на потенциальных предпринимателей и инвесторов. Именно поэтому в подходах к определению бизнес-моделей часто прослеживается технологическая составляющая.

Исследованию понятия «бизнес-модель» посвящены работы различных отечественных и зарубежных авторов. Так, В.Ю. Котельников утверждает, что в общем виде бизнес-модель является представлением о том, как должна выглядеть компания в настоящем и будущем; в ней должны быть отражены ключевые характеристики организации, логистические особенности, продукт или услуга, приносящие прибыль [5]. Дж. Линдер и С. Кантрелл в своем исследовании отметили, что бизнес-модель является основным способом создания стоимости, который можно представить по-разному, предпочтительнее использовать модель изменений — только с ее помощью компания может меняться со временем и оставаться прибыльной [5-8]. Одна из самых известных работ в исследуемой области принадлежит А. Остервальдеру и И. Пинье. Ученые считают, что бизнес-модель представляет собой комплекс, описывающий 9 направлений деятельности, которые характерны для любой организации [9].

Так как формирование понятия, типологизация моделей происходили на основе обобщения практического опыта предпринимательской деятельности, которому пытались придать теоретическую форму и основу, то на сегодняшний день существует несколько альтернативных подходов и к определению понятия бизнес-модели, и к типологизации: от универсальных до специфичных (применительно к определенным отраслям экономики) [1, 3, 5, 10-14].

Среди определений понятия бизнес-модели можно выделить две группы:

- в первой группе основной акцент делается на ценности, которая создается для клиентов, т.е. что и для кого мы создаем и возможно ли реализовать эту ценность потребителю с прибылью для компании;
- во второй группе – на внутренних процессах: как мы создаем ценность для клиентов (операционные процессы, исполнители процессов, их иерархия и зоны ответственности).

В первой группе определение бизнес-модели тесно связано с цепочкой создания ценности и ключевая характеристика модели – монетизация. Во второй группе определение бизнес-модели тесно связано с бизнес-процессами и ключевая характеристика модели – операционная эффективность. Оба подхода также связаны со стратегией компании: как реализуется деятельность компании, за счет чего достигаются ее цели [6].

Концепция бизнес-моделей призвана выработать язык для описания бизнеса с достаточной степенью детализации, чтобы были ясны ключевые моменты деятельности, но без лишних подробностей и частностей, которые специфичны для

конкретной реализации и уже не обладают необходимой степенью общности: достаточно подробные, чтобы быть инструментом для моделирования бизнеса, но не настолько кастомизированные, чтобы шаблоном было сложно воспользоваться для адаптации под конкретную бизнес-идею [11-15].

Бизнес-модель – это описание деятельности компании: организационной, операционной, финансовой, того, какой продукт/сервис/услугу компания предоставляет на рынке и как планирует свое развитие за счет трансформации механизмов функционирования и изменения предложения рынку результатов своей деятельности.

В свою очередь, бизнес-модель оператора подвижной связи имеет свои особенности, связанные с деятельностью организаций в инфокоммуникационной отрасли. Экономическим критерием отнесения деятельности организации к данной отрасли является доля основного вида деятельности. Так объем предоставляемых инфокоммуникационных услуг и технологий должен занимать более половины общих доходов компании [16]. Такой рынок имеет отличительные черты: высокая взаимозаменяемость услуг, общность потребностей в доступе к сетям и передачи информации, сетевой принцип построения сети связи, сетевые эффекты рынка, конвергентный характер развития [7, 11, 15, 16].

Кроме того, бизнес-модель должна учитывать, что организация вовлечена во внешнюю, внутри- и межотраслевую конкуренцию, должна модифицировать текущие услуги и создавать новые и осуществлять значительные вложения в поддержание и развитие сетей общего пользования.

Характеристика международных и российских стратегий развития цифровых продуктов и сервисов

Стратегия развития цифровых продуктов и сервисов является одним из определяющих этапов в создании успешной компании независимо от масштабов ее деятельности. Обусловлено это тем, что ни одна организация не в силах избежать естественного устаревания продукции, которое обусловлено действиями конкурентов и привыканием потребителей, что приводит к снижению объема продаж и потери выручки [1-3]. В условиях цифровой трансформации стратегия развития цифрового продукта или сервиса по сути является нулевым этапом в его жизненном цикле: еще ничего не существует, но уже необходимо заложить основы его реализации и успешности бизнеса.

По мнению российских ученых, стратегия развития цифрового продукта или сервиса состоит из 3 этапов:

1. Формирование видения продукта;
2. Определение целей;
3. Формирование концепции по его развитию [5, 7-10].

Для формирования видения продукта необходимо провести качественные и количественные исследования целевой аудитории, конкурентных предложений и рыночных трендов. Опираясь на полученную информацию, необходимо ответить на ряд вопросов:

- на каком географическом рынке будут продаваться цифровые услуги и сервисы; каковая целевая аудитория;
- каким потребительским свойствам должен отвечать цифровой продукт или сервис; какие функции будет выполнять; в чем потребительская ценность;
- в каком ценовом сегменте будет продаваться цифровой продукт или услуга;
- как он будет распространяться, через какие каналы; в чем ключевые особенности продвижения.

На основе ответов на вопросы и результатов проведенных исследований образуется первое видение продукта или сервиса, с учетом которого далее определяются цели. Под целями имеются в виду обозначенные достижения по распространению цифрового продукта или сервиса в заданный период времени.

После этого необходимо перейти к формированию концепции – понимания существующих потребностей целевой аудитории и их развития в ближайшей перспективе. Цифровой продукт или сервис должен обладать необходимыми свойствами для удовлетворения потребностей сейчас, которые можно будет модернизировать или трансформировать на протяжении всего жизненного цикла.

Ключевыми параметрами концепции развития цифрового продукта или сервиса российские исследователи называют [1, 5, 12-14, 17, 18]:

- разработка принципиального нового цифрового продукта или сервиса, имеющего уникальные свойства в связи с актуальными технологическими новациями и ожиданиями целевой аудитории;
- существенная модернизация существующего цифрового продукта или сервиса, значительное улучшение текущих потребительских свойств;
- модификация существующего цифрового продукта или сервиса для его использования на новых рынках (изменится география и целевая аудитория), изменение основных функциональных особенностей;
- изменения в ассортиментной политике: исключение цифровых продуктов и сервисов, не пользующихся спросом или оказывающих негативное влияние на доходность организации (акционные предложения).

Пристальная проработка стратегии развития цифрового продукта или сервиса необходима для успеха как в краткосрочной, так и долгосрочной перспективе. Пропуск одного из пунктов может привести к серьезным проблемам, вплоть до закрытия бизнеса в связи с убыточностью и банкротством.

Зарубежный подход к формированию стратегии развития цифрового продукта или сервиса имеет схожие и отличительные черты. По мнению Р. Пихлера, стратегию необходимо рассматривать во взаимосвязи (рис. 1) с дорожной картой продукта: стратегия развития цифрового продукта или сервиса описывает путь достижения долгосрочной цели (включая ценностное предложение, целевую аудиторию, ключевые характеристики продукта), а дорожная карта отражает, как стратегия реализуется на практике с учетом конкретных сроков [19]. Дорожная карта представляет собой схематичное изображение, где каждый этап стратегии последовательно связан друг с другом. Перейти на следующий этап можно только по завершении предыдущего. Бэклог продукта – это перечень основных требований к продукту и задач, расставленных в порядке приоритета.

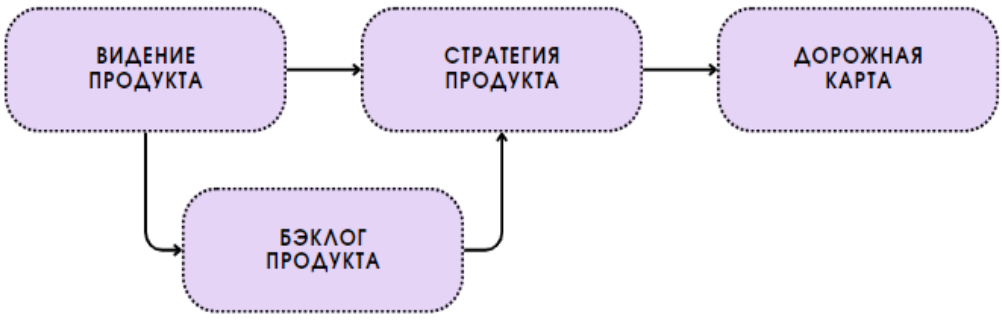

Рисунок 1

Сама по себе стратегия развития цифрового продукта или сервиса является высокоуровневым планом, который направлен на реализацию видения продукта и ключевой цели. Стратегия призвала объяснить: для кого предназначен продукт, почему его захотят купить и использовать, что собой представляет цифровой продукт или сервис и чем он кардинально отличается от других, а также почему компании целесообразно инвестировать именно в него.

Ключевые элементы продуктовой стратегии (стратегии развития цифрового продукта или сервиса) отражены на рис. 2. Это важные аспекты продукта или сервиса, которые имеют решающее значение для создания ценности: именно они побеждают потребителя выбрать товар среди конкурирующих предложений. Необходимо перечислить не все характеристики, а лишь 3-5 основных, оказывающих влияние на решение человека о покупке и использовании цифрового продукта или сервиса.

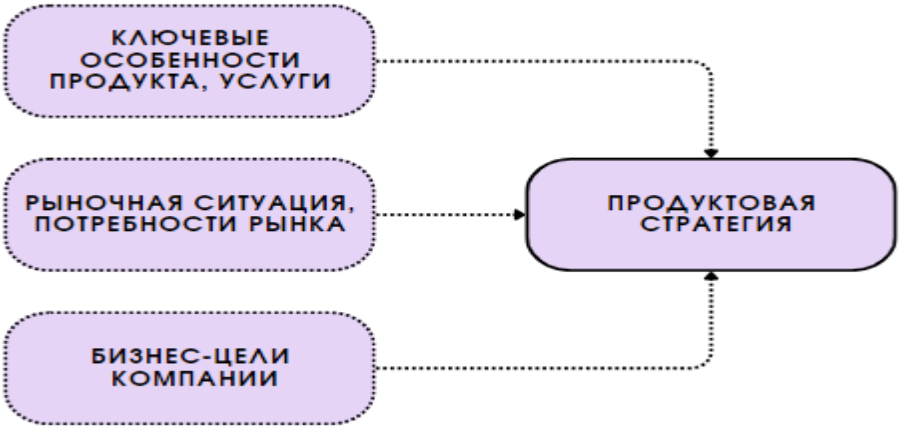

Рисунок 2

Бизнес-цели должны отражать то, как продукт или сервис принесет пользу компании, почему стоит инвестировать именно в него. Необходимо определить, принесет ли продукт или сервис доход, снизит ли затраты на производство, повысить ли узнаваемость бренда. Четкое определение бизнес-целей позволит выбрать правильные ключевые показатели эффективности (*KPI*) для оценки продукта. Зарубежные исследователи отмечают, что стратегия развития цифрового продукта или сервиса – это не четко зафиксированный план, он должен меняться по мере роста и становления продукта. Необходимо регулярно пересматривать и корректировать стратегию. Некоторые авторы полагают, что оптимально это делать не реже 1 раза в квартал.

Таким образом, существуют различные подходы к формированию стратегии развития цифровых продуктов и сервисов. Российские и международные исследователи сходятся в том мнении, что стратегии обязательно должна включать в себя такие разделы как «видение продукта» и «бизнес-цели», «целевая аудитория».

В то же время, существуют отличительные черты: российские маркетологи полагают, что стратегия развития цифрового продукта или сервиса является независимым «проектом», в то время как зарубежные ученые настаивают на том, что стратегия должна существовать во взаимосвязи с дорожной картой продукта [14].

Предлагаемые методические подходы по формированию стратегии развития цифровых продуктов и сервисов

Цифровая трансформация экономики привела к значительным бизнес-изменениям: если раньше организации продавали физические товары (продукты), то сейчас и они стали цифровыми.

Под цифровым продуктом следует понимать совокупность физических объектов и цифровых процессов [15, 17, 18]. Сейчас компании вынуждены продавать не просто товар, а еще и набор технологий, который с ним связан. Цифровой продукт получает дополнительную ценность для потребителя. Под цифровым сервисом можно понимать информационный ресурс, созданный для удовлетворения определенных потребностей человека [12]. Они призваны не только виртуализировать бизнес-процессы организации, но и создать новый способ конкуренции.

Все цифровые сервисы обладают общими характеристиками:

- в полной мере удовлетворяют определенные запросы целевой аудитории;
- свободный доступ: каждый может использовать сервис в удобное время;
- доступность: для использования цифрового сервиса можно использовать практически любое устройство, подключенное к сети интернет;
- адаптивность к потребностям: сервис можно изменять, добавлять новые функции, необходимые для организации или потребителей;
- универсальность: цифровой сервис можно интегрировать в работу любого структурного подразделения;
- удобство в использовании: если сервис неудобный, появится обратная связь от клиентов или его пользователей.

Все цифровые продукты и сервисы основаны на новых технологиях, но новейшие технологии 5*G* и 6*G* позволят использовать новые: искусственный интеллект, машинное обучение, технологии дополненной и виртуальной реальности, большие данные, Интернет вещей, что должно учитываться при формировании стратегии цифрового продукта или сервиса [17-20].

Стратегия развития цифрового продукта или сервиса (или продуктовая стратегия) – это долгосрочный план действий, направленный на достижение поставленной в организации цели, хотя ее формат может быть любым: кто-то создает презентацию, делает заметки в «облаке» или формирует отдельный документ. Это зависит от масштабов компании и требований руководства.

Основная задача продуктовой стратегии – всегда держать фокус на достижении цели. С развитием цифрового продукта или сервиса будет приходить обратная связь от целевой аудитории с просьбами добавить новые функции или внести какие-то изменения. Необходимо тщательно анализировать возможные изменения: добавить новые функции — не значит приблизиться к достижению цели.

Разработку продуктовой стратегии предваряю: определение миссии компании – то, какие изменения она хочет привнести в мир и стратегии компании – то, как организация будет реализовывать миссию. После это составляется продуктовая стратегия – часть основной стратегии компании (рис. 3).

WHAT (ЧТО)	ЧТО ХОЧЕТ ПОТРЕБИТЕЛЬ? КАКИМИ ХАРАКТЕРИСТИКАМИ И ФУНКЦИЯМИ ДОЛЖЕН ОБЛАДАТЬ ЦИФРОВОЙ ПРОДУКТ ИЛИ СЕРВИС?
WHO (КТО)	КТО ЗАХОЧЕТ ПРИОБРЕСТИ НАШ ЦИФРОВОЙ ПРОДУКТ ИЛИ СЕРВИС? КАКИМИ ХАРАКТЕРИСТИКАМИ ОБЛАДАЕТ?
WHY (ПОЧЕМУ)	ПОЧЕМУ ПОТРЕБИТЕЛЬ ЗАХОЧЕТ ПРИОБРЕСТИ НАШ ЦИФРОВОЙ ТОВАР ИЛИ СЕРВИС? КАКИЕ ПОТРЕБНОСТИ ОН ЗАКРОЕТ?
WHEN (КОГДА)	КОГДА ПРОИЗОЙДЕТ ПОКУПКА? ОНА БУДЕТ РАЗОВАЯ ИЛИ ПЕРИОДИЧЕСКАЯ?
WHERE (ГДЕ)	ГДЕ БУДЕТ ПРОИЗВЕДЕНА ПОКУПКА? КАКОЙ КАНАЛ РАСПРЕДЕЛЕНИЯ БУДЕТ ВЫБРАН?

Рисунок 3

Формирование стратегии развития цифрового продукта или сервиса можно разбить на 5 основных этапов:

1. Определение цели.
2. Проведение исследований, сбор информации.
3. Формирование концепции, дифференциация предложения.
4. Составление списка задач по достижению цели, приоритезация задач.
5. Формирование единого плана и его оценка.

После определения цели можно выбрать определенный вид продуктовой стратегии из пяти вариантов или их комбинации:

1. Стратегия поиска: подходит для запуска стартапа, разработки нового продукта или сервиса, входа на еще несформированный или нестабильный рынок, развития инновационного продукта. Основная цель такой стратегии заключается в поиске баланса между функциями созданного продукта и потребностями целевой аудитории.

2. Стратегия роста: подходит для развития уже существующих цифровых продуктов и сервисов. Основная цель заключается в росте коэффициента привлечения пользователей и снижении их оттока.

3. Стратегия «пивот» (англ. *pivot* – вращение, поворот): применяется, когда продукт не удовлетворяет ожидания клиентов или были значительные изменения на рынке. Основная цель – изменить ключевые характеристики, переосмыслить существующее предложение

4. Стратегия оптимизации: подходит, когда цифровой продукт или сервис достиг стадии зрелости и его рост замедлился. Основная цель – улучшить текущие показатели, доработать ключевые маркетинговые процессы, укрепить командный дух.

5. Стратегия масштабирования: подходит на той же стадии продукта, что и стратегия оптимизации, но ее ключевое отличие в том, что улучшение показателей будет достигнута через покорение новых рынков и дальнейшего расширения. Масштабирование не всегда связано с географией, возможно сделать упор на другие целевые аудитории.

В основе формирования стратегии развития цифрового продукта или сервиса лежат следующие три методических принципа. Первый – определение целевой аудитории включает в себя несколько этапов: ответы на вопросы по методике «5*W*» (рис. 3) и детализацию результата по социально-демографическим, географическим, психографическим, поведенческим характеристикам (рис. 4).

СОЦИАЛЬНО-ДЕМОГРАФИЧЕСКИЕ	СТРАНА, ГОРОД
ГЕОГРАФИЧЕСКИЕ	ИНТЕРЕСЫ, ХОББИ, ИНФЛЮЕНСЕРЫ, СМИ, БРЕНДЫ
ПСИХОГРАФИЧЕСКИЕ	ОТНОШЕНИЕ К КОМПАНИИ, ОТНОШЕНИЕ К ЦИФРОВОМУ ТОВАРУ ИЛИ СЕРВИСУ, МОТИВАЦИЯ К ПОКУПКЕ И ЕЕ ПЕРИОДИЧНОСТЬ
ПОВЕДЕНЧЕСКИЕ	ПОЛ, ВОЗРАСТ, РОД ДЕЯТЕЛЬНОСТИ, СЕМЕЙНОЕ ПОЛОЖЕНИЕ, УРОВЕНЬ ДОХОДА, ОБРАЗОВАНИЕ

Рисунок 4

Второй принцип охватывает вопросы исследования рынка, а именно:

- определение его емкости;
- изучение аналитических прогнозов;
- проведение *SWOT*-, *PESTEL*-анализов (рис. 5 и 6);
- использование модели «5 сил» М. Портера (рис. 7).

Рисунок 5

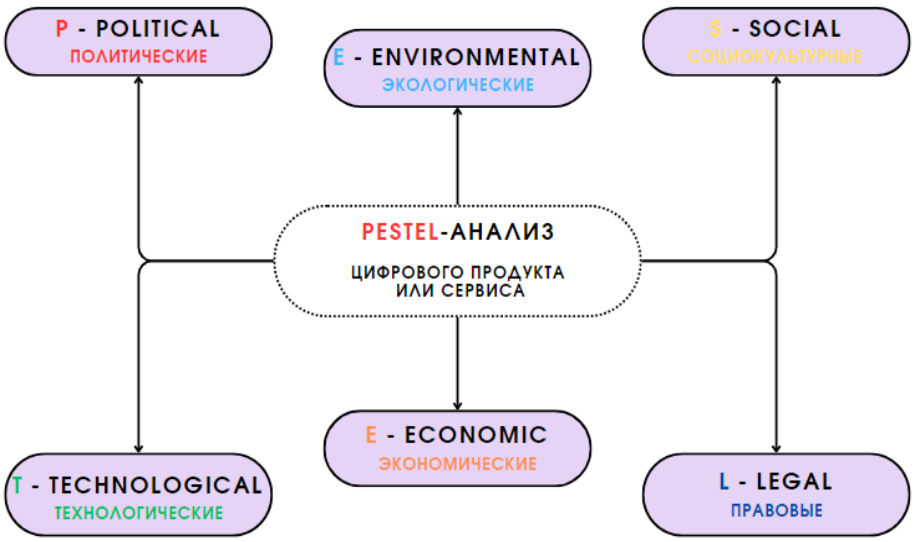

Рисунок 6

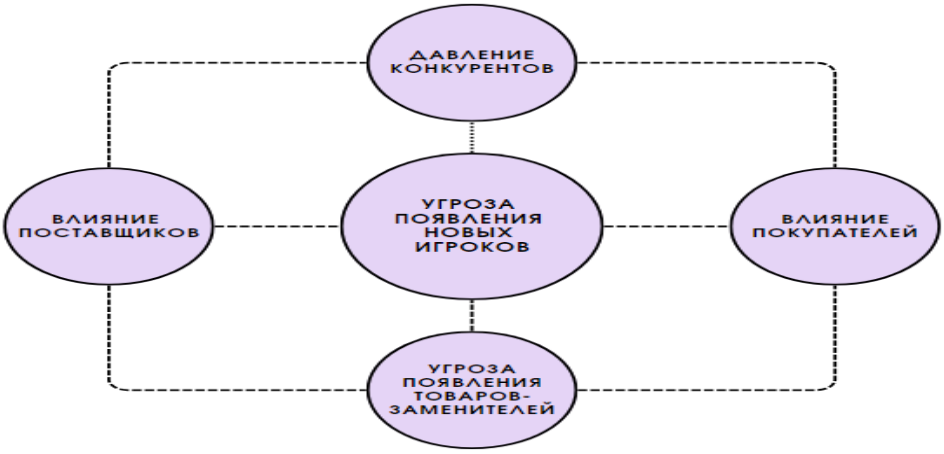

Рисунок 7

Третий принцип состоит в анализе цифрового продукта или сервиса посредством проведения *VRIO*-анализа (рис. 8) и определения ключевых функций, цены, каналов распространения.

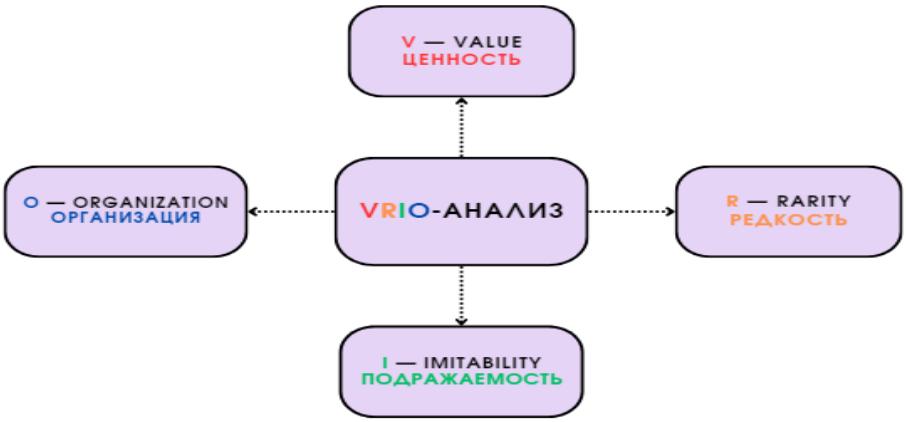

Рисунок 8

На основании полученных данных следует сделать выводы и сформировать необходимую концепцию развития цифрового продукта или сервиса (рис. 9).

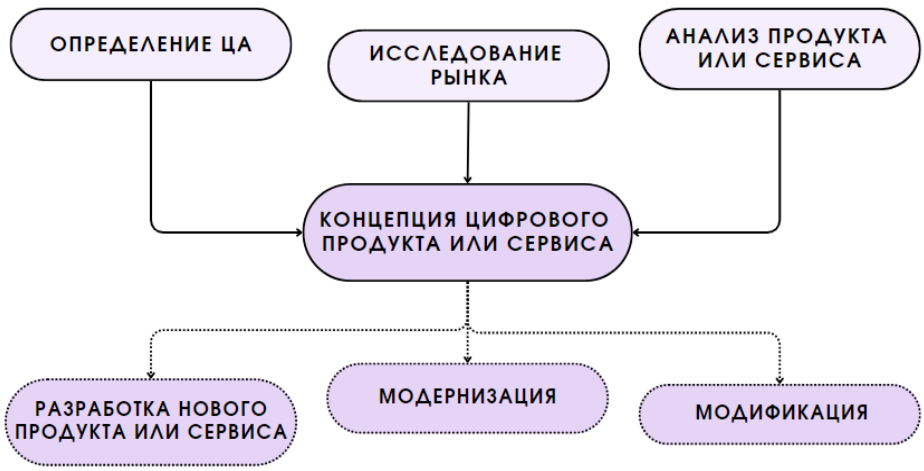

Рисунок 9

Заключение

Изменения в бизнес-моделях организаций, обусловленные цифровой трансформацией экономики, привели к необходимости формирования стратегии развития цифровых продуктов и сервисов.

Ввиду появления новых технологий, развития социальных сетей, изменений в потребительском поведении, авторами предложена новые методические рекомендации по формированию стратегии, включающие в себя несколько этапов: определение целевой аудитории, исследование рынка, анализ цифрового продукта или сервиса.

В условиях быстроты развития цифровых продуктов или сервисов проведенное исследование указывает на целесообразность дополнения изложенной концепции следующими этапами: модернизация, модификация или разработка принципиально нового решения.

Литература

1. Акатов Н.Б. Бизнес-модели и их применение в управлении инновационным саморазвитием компании: учебно-методическое пособие. Под редакцией А.В. Молодчик. – Пермь: Пермский национальный исследовательский политехнический университет, 2012. – 196 с.
2. Афоничкина Е.А., Бахарев Н.П., Лихацкая А. Анализ и оценка конкурентных преимуществ предприятия // Вестник ВУиТ, 2009. – № 17. URL: https://cyberleninka.ru/article/n/analiz-i-otsenka-konkurentnyh-preimuschestv-predpriyatiya.
3. Каз Е.М., Краковецкая И.В., Нехода Е.В., Редчикова Н.А. Бизнес-модели компаний и устойчивое развитие. Под редакцией Е.В. Неходы. – Томск: Издательство Томского государственного университета, 2020. – 214 с.
4. Борисова О.В. Основные тенденции развития цифровой экономики // РИСК: Ресурсы, информация, снабжение, конкуренция, 2019. – № 1. – С. 128-131.
5. Котельников В.Ю. Новые бизнес-модели для новой эпохи быстрых перемен, движимых инновациями. – М.: Эксмо, 2007. – 96 с.
6. Вайл П. Цифровая трансформация бизнеса: Изменение бизнес-модели для организации нового поколения / Питер Вайл, Стефани Ворнер; перевод И. Окунькова. – Москва: Альпина Паблишер, 2019. – 264 с.
7. Кузовкова Т.А. Цифровая трансформация экономики: учебное пособие / Т.А. Кузовкова, О.И. Шаравова. – Москва: Ай Пи Ар Медиа, 2023. – 140 с.
8. Грибанов Ю.И. Цифровая трансформация бизнеса: учебное пособие / Ю.И. Грибанов, М.Н. Руденко. – 2-е изд. – Москва: Дашков и К, 2021. – 214 с. – ISBN 978-5-394-04192-1.
9. Данько Т.П., Китова О.В. Вопросы развития цифрового маркетинга // ПСЭ. – 2013. – № 3 (47). URL: https://cyberleninka.ru/article/n/voprosy-razvitiya-tsifrovogo-marketinga.
10. Егина Н.А. Трансформация модели поведения потребителя в условиях цифровой экономики // Финансы и кредит, 2019. – Т. 25. – В. 9. – С. 1971-1986.
11. Женчур М.А., Платунина Г.П., Громова М.О. Цифровая трансформация компании // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 49-й Международной конференции. Москва, 2022. – С. 58-62.
12. Зараменских Е.П. Цифровые сервисы: их атрибуты и взаимосвязь с архитектурой предприятия // Вестник ГУУ, 2018. – № 10. URL:

https://cyberleninka.ru/article/n/tsifrovye-servisy-ih-atributy-i-vzaimosvyaz-s-arhitekturoy-predpriyatiya.
13. Гиротра К. Оптимальная бизнес-модель: четыре инструмента управления рисками / Гиротра Каран, С. Нетесин; перевод М. Брандес. – Москва: Альпина Паблишер, 2019. – 216 с.
14. Колосова Д.М., Кузьмин К.А., Лебедь В.Е. Основы цифрового маркетинга // Экономика и бизнес: теория и практика, 2022. – № 11-1. URL: https://cyberleninka.ru/article/n/osnovy-tsifrovogo-marketinga
15. Кузовкова Т.А., Кузовков А.Д., Шаравов И.М. Понятие ценности цифровых платформ и методы оценки синергии их эффективности // Электронный научный журнал «Век качества», 2022. – № 3. – С.73-96.
16. Кузовкова Т.А., Салютина Т.Ю., Шаравова О.И. Формирование цифровой экосистемы бизнеса / Учебное пособие для магистрантов. – М.: ООО Компания «Ай Пи Эр Медиа», 2022. – 122 с.
17. Кузовкова Т.А., Алмаева О.П., Вольнов А.А., Шаравов И.М. Реализация сценариев использования технологий на базе сетей пятого поколения // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 47-й Международной конференции. Москва, 2021. – С. 30-33.
18. Кузовкова Т.А., Девяткин Е.Е., Тихвинский В.О., Шаравова О.И. Перспективы развития цифровых услуг интеллектуального мира на основе сетей подвижной связи новых поколений // РИСК: Ресурсы, Информация, Снабжение, Конкуренция, 2022. – № 2. – С. 80-86.
19. Кузовкова Т.А., Кузовков Д.В., Шаравова О.И. Характеристика мирового развития цифровой экономики и уровня цифрового развития России // В сборнике: Технологии информационного общества. Материалы XIII Международной отраслевой научно-технической конференции, 2019. – С. 133-135.
20. Гришина С.А. Стратегический менеджмент: проектный подход: учебное пособие / С.А. Гришина, А.Н. Шишкин. – Тула: Тульский государственный педагогический университет имени Л.Н. Толстого, 2020. – 184 с.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ЦИФРОВОЙ ЭКОСИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕССНОЙ АНАЛИТИКИ

Р.Ю. Уманский, *к.э.н., доцент, Московский технический университет связи и информатики, rumanskiy@mail.ru;*
С.Д. Борисов, *Московский технический университет связи и информатики, sd.borisov@gmail.com.*

УДК 338.2

Аннотация. Статья посвящена исследованию возможностей технологии процессной аналитики по повышению эффективности деятельности цифровой экосистемы. Рассмотрена эволюция процессной аналитики и основные тенденции в ее развитии. Представлены основные характеристики цифровой экосистемы и на практических примерах рассмотрен алгоритм анализа процессов цифровой экосистемы и сформулированы выводы по результатам обследования.

Ключевые слова: процессная аналитика; мультипроцессная аналитика; цифровая экосистема; эффективность деятельности; моделирование процессов.

IMPROVING THE PERFORMANCE OF DIGITAL ECOSYSTEM USING PROCESS MINING

R.Yu. Umanskiy, *Ph. D. in Economics, associate Professor, Moscow Technical University of Communications and Informatics;*
S.D. Borisov, *Moscow Technical University of Communications and Informatics.*

Annotation. The article is devoted to the study of the possibilities of process mining technology to improve the efficiency of the digital ecosystem. The evolution of process mining and the main trends in its development are considered. The main characteristics of the digital ecosystem are presented and an algorithm for analyzing the processes of the digital ecosystem is considered using practical examples and conclusions based on the results of the survey are formulated.

Keywords: process mining; object-centric process mining; digital ecosystem; performance; process modeling.

Введение

Одной из важнейших целей выработки и реализации стратегии развития в условиях цифровой экономики остается поиск направлений в оптимизации существующих издержек и повышение внутренней эффективности процессов организации. В условиях цифровой трансформации бизнеса проблема повышения внутренней эффективности становится особенно актуальной при формировании цифровых экосистем как сложно структурированных организаций, которые ведут свою деятельность на разнообразных высококонкурентных сегментах рынка и имеющих масштабную организационную структуру с огромным количеством внутренних процессов [1].

В цифровых экосистемах на первый план, помимо вопросов оптимизации расходов и повышения лояльности клиентов, начинают выходить проблемы, связанные с эффективной координацией внутренних процессов по созданию и продвижению различных цифровых продуктов, а также их интеграции в единый эффективный механизм управления продуктами и услугами в цифровой экосистеме. Значительный рост предлагаемых в рамках цифровой экосистемы продуктов и услуг, зачастую не связанных между собой, ставит перед менеджментом задачу выстроить управление в цифровой экосистеме таким образом, чтобы процессы разработки и продвижения продуктов и сервисов были не просто регламентированы и упорядочены, но и полностью прозрачны и достоверны для принятия эффективных управленческих решений по их совершенствованию, а в условиях цифровой среды – даже нередко оптимизированы без участия человеческого фактора [2].

В связи с этим в цифровых экосистемах необходимо внедрять принципиально новые инструменты анализа внутренних процессов в цифровой среде, которые должны автоматизировать исследование протекающих внутренних процессов и на основе полученных данных строить имитационные модели эталонного процесса и давать рекомендации менеджменту на корректировочные воздействия. Среди таких инструментов, позволяющих исследовать «цифровые следы» реальных процессов в информационных системах и устранить их неэффективность, выделяется технология процессной аналитики (анг. *Process Mining*).

Развитие концепции и прикладного инструментария процессной аналитики

Как отмечалось выше, одним из наиболее современных подходов в области анализа процессов и построения моделей оптимальной последовательности принятия решений является технология процессной аналитики [3, 4], занимающаяся изучением алгоритмов принятия решений на основе их «цифрового следа». Под термином «цифровой след» будем понимать совокупность зарегистрированных в любых внутренних цифровых учетных системах и электронных журналах организации воздействий субъектов принятия решений на уникальный объект принятия решений в процессе его прохождения по цепочке согласования [5].

До настоящего момента на протяжении более чем 100 лет подходы к анализу и оптимизация внутренних процессов организаций естественным образом эволюционировали от теории научного управления Фредерика Тейлора до совокупности детально изученных и описанных классических способов анализа: анкетирование, опросы экспертов, хронометражи, моделирование, использование статистических методов управления процессами, *Six sigma* и др. И только с момента начала повсеместного развития цифровых технологий, роботизации, интернета вещей появилась основа для качественно нового этапа исследования и оптимизации процессов с использованием технологии процессной аналитики.

Основателем технологии процессной аналитики считается профессор Вил ван дер Аалст из технического университета Эйндховена [6, 7], исследования которого в начале 2000-х стали основой для развития комплексного методологического и технологического развития решений в данной области [8].

Активное развитие инновационных цифровых технологий, приведшее к трансформации бизнес-моделей работы компаний, а также интенсивная разработка и внедрение в практическую сферу платформенных решений и новых компетенций работы сотрудников в цифровой среде привело к тому, что технология процессной аналитики сейчас активно приходит на смену классическим «ручным» методам описания и моделирования процессов через проведение бизнес-аналитиками интервью участников процесса и последующим моделированием его в виде графической модели [9, 10]. В цифровых экосистемах, работающих на платформенных решениях, все процессы усложняются и ускоряются, а также резко растет количество участников каждого процесса и связей между ними. При этом с учетом массовой цифровизации всех процессов количество используемых и накапливаемых данных растет по экспоненте, а инструменты процессной аналитики позволяют охватить все вариации и мелкие шаги внутри каждого процесса, восстановить реальный процесс на миллионах событий по «цифровым следам». После объективного отображения реального процесса с любыми вариациями и отклонениями процессная аналитика позволяет выявить узкие места, неэффективность и принять решения по оптимизации и улучшению клиентского опыта.

Следует отметить, что, несмотря на то, что процессная аналитика – абсолютно новая технология, возникшая на стыке исследования данных (анг. *Data Mining*) и бизнес-аналитики (анг. *Business Intelligence*), ее активное применение растет как во всем мире, так и в России [11, 12]. В связи со своим широким практическим применением и стремительно реализуемой цифровой трансформацией компаний в различных отраслях, инструментарий процессной аналитики также качественно эволюционирует и развивается уже в специфических прикладных направлениях. Так, одним из самых современных и продвинутых ответвлений процессной аналитики можно считать мультипроцессную аналитику

[13, 14]. Ее особенность заключается в более широком, по сравнению с классическим инструментарии процессной аналитики, возможностью по оптимизации связанных процессов. Как было описано ранее, классический анализ процессов базируется на изучении всех шагов одного процесса, построении его эталона и моделировании сценариев его оптимизации на основе вероятностей возможных отклонений. Технология мультипроцессной аналитики предлагает пользователю рассмотреть одновременно несколько связанных между собой процессов и оптимизировать их как одно целое. Для этого в рамках мультипроцессной аналитики строится объектно-ориентированная математическая модель процессов, предусматривающая несколько типов взаимосвязей, входящих в нее объектов: «один ко многим», «многие ко многим». Такой подход предоставляет возможность сравнить несколько взаимосвязанных событий в последовательных процессах относительно друг друга и проанализировать эффективность пути между ними. Такое масштабное изменение в подходе должно привести к появлению новых и переосмыслению существующих возможностей по анализу процессов.

Также как и для классической процессной аналитики, преимущества мультипроцессной аналитики можно кратно масштабировать на предприятиях, для внутренних процессов которых характерны массовость, высокая частота и регулярность. И, конечно, для создания карты путей процессов обязательным условием применения мультипроцессной аналитики является наличие цифровых следов операций. Все указанные условия выполнимы для интенсивно развивающихся цифровых экосистем.

Кроме активного развития мультипроцессной аналитики, можно отметить активное использование технологий искусственного интеллекта, машинного обучения и больших языковых моделей в области анализа и оптимизации процессов, которые в ближайшие годы смогут значительно повысить достигаемые в результате использования процессной аналитики эффекты за счет того, что данные технологии смогут самостоятельно не только искать проблемы и возможности в процессах, но и предлагать решения проблем для повышения эффективности и создания дополнительной ценности [15, 16]. Используя преимущества инструментов процессной аналитики, возможно резко повысить эффективность в тех областях, в которых раньше это было сделать достаточно сложно (медицина, телекоммуникации, крупные сложноструктурированные холдинговые структуры и т.д.).

Основные характеристики цифровых экосистем и стратегические возможности применения процессной аналитики для повышения их эффективности

Как уже отмечалось выше, появление новых цифровых технологий привело к требованию цифровизации большинства процессов и услуг в различных отраслях и сформировало новые платформенные бизнес-модели взаимодействия производителей и потребителей с появлением цифровых экосистем [17]. Если рассматривать цифровую экосистему как вариант интегрированной комплексной организации бизнеса [18], основанный на создании потребительской ценности на базе множества взаимосвязанных цифровых сервисов и продуктов, представленных на общей платформе, то можно выделить следующие форматы ее организации:

- зонтичный – предполагающий наличие базового цифрового продукта или сервиса и построение нескольких организационно-зависимых дополнительных к нему сервисов на базе единой платформы;

- горизонтальный – предполагающий создание цифрового пространства, действующего по принципу маркетплейса, куда имеют доступ множество независимых поставщиков цифровых продуктов и услуг;
- гибридный – сочетающий в себе характеристики обоих представленных вариантов. Это – открытая для внешних поставщиков цифровая экосистема, ядром которой может быть единый набор сервисов. Внешние поставщики цифровых услуг обязательно удовлетворяют набору критериев центрального оператора экосистемы, поскольку их сервис представляется от имени его бренда.

Исходя из такого понимания, цифровая экосистема способна предоставить бизнесу ряд уникальных конкретных преимуществ в виде:

- единого потока контактов с клиентами в цифровых каналах, себестоимость привлечения которых сокращается в результате эффекта масштаба;
- синергетического эффекта от объединения нескольких услуг и создание широкой клиентской ценности;
- стратегической возможности аллоцировать свободный капитал в потенциально перспективные направления развития бизнеса.

Ключевыми элементами цифровой экосистемы являются применяющиеся в ее контуре технологические решения, обеспечивающие возможность омниканального взаимодействия с клиентами и синхронизацию внутренних процессов. К таким решениям можно отнести следующие:

- наличие единой цифровой платформы, на базе которой возможно организовать интеграцию нескольких цифровых сервисов;
- сервисы по интеграции для поставщиков цифровых услуг, представленных на платформе;
- технология сквозной идентификации клиентов, обеспечивающая бесшовный обмен информацией о клиенте и для клиента в процессе формирования предложения.

В цифровой экосистеме целевой результат контакта с потенциальным клиентом предполагает формирование ценностного предложения на основе оптимального набора из нескольких продуктов. При этом для максимизации отдачи от контакта экосистема должна сформулировать свое продуктовое предложение с учетом:

- базового продукта или услуги, за которым обратился потенциальным клиент;
- адекватного набора комплементарных цифровых продуктов экосистемы, подобранных с учетом индивидуальных характеристик данного потребителя и жизненной ситуации;
- минимального времени на формирование такого предложения (здесь и сейчас).

Зонтичная структура цифровой экосистемы часто предполагает наличие совершенно разных продуктовых предложений, формируемых под базовым продуктом, реализуемым материнской компанией. При такой схеме взаимодействия несколько независимых компаний-участников общей цифровой экосистемы должны синхронизировать свои продуктовые предложения в каждой точке контакта клиента с любым продуктом экосистемы. Сложная схема взаимодействия еще более усложняется при разрозненных независимых процессах

обработки клиентского запроса в каждой из компаний, входящих в цифровую экосистему. В таких условиях критическую важность приобретает эффективность отработки внутренних алгоритмов и качественную поставку целевого набора ценностей экосистемы к клиенту.

Одним из классических примеров ситуации, в которой клиенту может быть продано несколько связанных продуктов цифровой экосистемы (на примере Сбера) является запрос клиента на поиск жилья на вторичном рынке для покупки. Во время контакта с клиентом в цифровом канале (платформа ДомКлик) цифровая экосистема имеет возможность предложить потенциальному покупателю пакет собственных цифровых продуктов, в зависимости от его потребностей:

- поиск объекта жилья и помощь в проведении сделки (в данном примере базовая ценность, предоставляемая за комиссионное вознаграждение компанией ДомКлик, дочерней структуры Сбера);
- ипотечный кредит на приобретение жилья на вторичном рынке (комплементарная ценность, процентный доход, ПАО Сбербанк);
- кредитная карта, необеспеченный потребительский кредит (комплементарная ценность, процентный доход, ПАО Сбербанк);
- страхование жилья (комплементарная ценность, страховая премия СК Сбербанк Страхование, дочерняя структура Сбера);
- услуги по формированию документов на имущественный налоговый вычет, оформление и использования материнского капитала (комиссионное вознаграждение, СберРешения, дочерняя структура Сбера);
- услуги и товары для ремонта на маркетплейсе (агентское вознаграждение, СберМаркет, дочерняя структура Сбера) и т.д.

Обратим внимание, что первичной точкой контакта может быть любая из перечисленных компаний экосистемы, а целевой набор ценности аналогичен. В ситуации, когда клиент принимает решение приобрести набор продуктов цифровой экосистемы, запускается набор независимых процессов, результатом которых будет являться онлайн- или офлайн-поставка ценности. Успешная и своевременная отработка процессов поставки позволит конвертировать контакт с клиентом в реальную продажу. Наряду с задачей синхронизации независимых процессов не менее актуально стоит вопрос о снижении их себестоимости: ее решение напрямую влияет на рентабельность активов компаний – участников цифровой экосистемы.

Представим на рис. 1 упрощенный пример гипотетически протекающих на предприятиях экосистемы процессов, связанных с одним общим запросом клиента и призванных доставить для него два различных цифровых продукта экосистемы.

Данный пример в явном виде демонстрирует не только параллельное протекание нескольких клиентских процессов в экосистеме, но и их взаимозависимость: только после финального выбора объекта сделки на шаге 4.2 для клиента могут быть определены окончательные условия по комплементарным продуктам (ипотечный кредит, страхование залога и жизни заемщика) 5.3 и 6. Таким образом, любая неоптимальность на смежных шагах процесса приводит либо к задержке по формированию комплементарной ценности для клиента, либо к его некорректной формулировке, что в свою очередь снижает вероятность конвертации контакта с клиентом в продажу и сокращает рентабельность сделки.

Уникальной характеристикой цифровой экосистемы является, с одной стороны, наличие общей для всех продуктов цифровой платформы для первичного контакта с клиентом и, с другой стороны, цифровой характер процессов, связывающих операции внутри экосистемы. Наличие цифровых следов по ключевым процессам создает идеальные условия для использования инструмента

процессной аналитики с целью выявления неоптимальных участков регулярных процессов, их оптимизации и спрямления.

Рисунок 1

Исследование практических результатов анализа связанных процессов с использованием технологии процессной аналитики

Рассмотрим пример применения инструментария процессной аналитики для поиска неоптимальности процедуры обработки клиентской информации в цифровой экосистеме.

В представленной в предыдущем разделе схемы действия параллельных процессов (4 и 5) окончательного определения параметров для сделки купли-продажи объекта недвижимости (шаг 4.2) и формирования индивидуального предложения по ипотечному кредиту на его покупку (шаг 5.2) присутствует вложенный подпроцесс обмена информацией. Данный подпроцес связывает продажу двух взаимозависимых цифровых продуктов клиенту и должен обеспечить своевременную передачу клиентских данных между отдельными центрами компетенций экосистемы по следующему алгоритму:

1. На стороне процесса подбора объекта недвижимости формируется анкета, отражающая финальные условия покупки.
2. Карточка сделки и анкета клиента загружаются в систему *CRM*.
3. Оператор/алгоритм определяет связанные со сделкой процессы и маршрутизирует анкету в параллельный процесс после проверки корректности заполнения данных.

4. Запускается процесс расчета индивидуальных условий по ипотечному кредиту для приобретения выбранного объекта недвижимости.

5. Предложение по кредиту передается в анкету клиента для формирования предложения.

6. Предложение передается клиенту в рамках параллельного процесса оформления сделки купли-продажи.

Для проведения анализа протекающих процессов с использованием технологии процессной аналитики воспользуемся следующим алгоритмом действий:

1. **Первый этап** состоит из подготовки необходимых для анализа данных. На этом шаге требуется определить, какие информационные системы организации задействованы на этапе обработки процесса контакта с клиентом, таких систем может быть несколько. В целевых информационных системах нужно настроить сквозную идентификацию каждого уникального экземпляра процесса (контакта с клиентом и последующих действий до продажи продукта), который должен иметь собственный номер. После настройки сквозной нумерации экземпляров готовится выгрузка данных по всем доступным экземплярам процесса, глубина выгрузки данных должна обеспечивать возможность отследить повторения процесса не менее 10 раз. Чем больше повторений процесса будет доступно, тем более точными будут последующие расчеты. Учитывая особенность постановки задачи (найти оптимальный канал продаж), при подготовке данных обязательно нужно в явном виде разделить все экземпляры процесса по каналам продаж, в которых они осуществляются. Важно выгрузить из внутренних систем компаний также все необходимые для тестирования нашей гипотезы дополнительные данные. Например, если от размера чека в заказе зависит алгоритм и количество этапов его согласования, такие данные также будут полезными.

После выгрузки данных они передаются для обработки в специализированный программный комплекс, отвечающий за построение процессной аналитики.

2. **Второй этап** предполагает анализ полученных данных. С помощью платформы процессной аналитики построена карта процесса в виде графа, определены основные шаги и количество входов и выходов экземпляров процесса, которые были загружены на первом этапе. На данном шаге очень полезно провести верификацию фактической карты процесса с той, которая предусмотрена внутренними нормативными документами организации, и установить наличие возможных отклонений. На рис. 2 представлен в графическом виде цифровой след указанного процесса.

По итогам построения графа процесса с помощью инструментария по процессной аналитике можно провести детальный анализ процесса для каждого из имеющихся каналов продаж. Для этого требуется разработать перечень аналитических количественных индикаторов качества процесса (метрики) и рассчитать их значения для каждого из каналов продаж и периода. Чаще всего анализируются длительность процесса и его успешность. В качестве меры успешности можно выбрать операцию, которая в логике анализируемого процесса означает успешное достижение результата (например, подписание договора, поставка товара заказчику, выдача кредита, страхование риска).

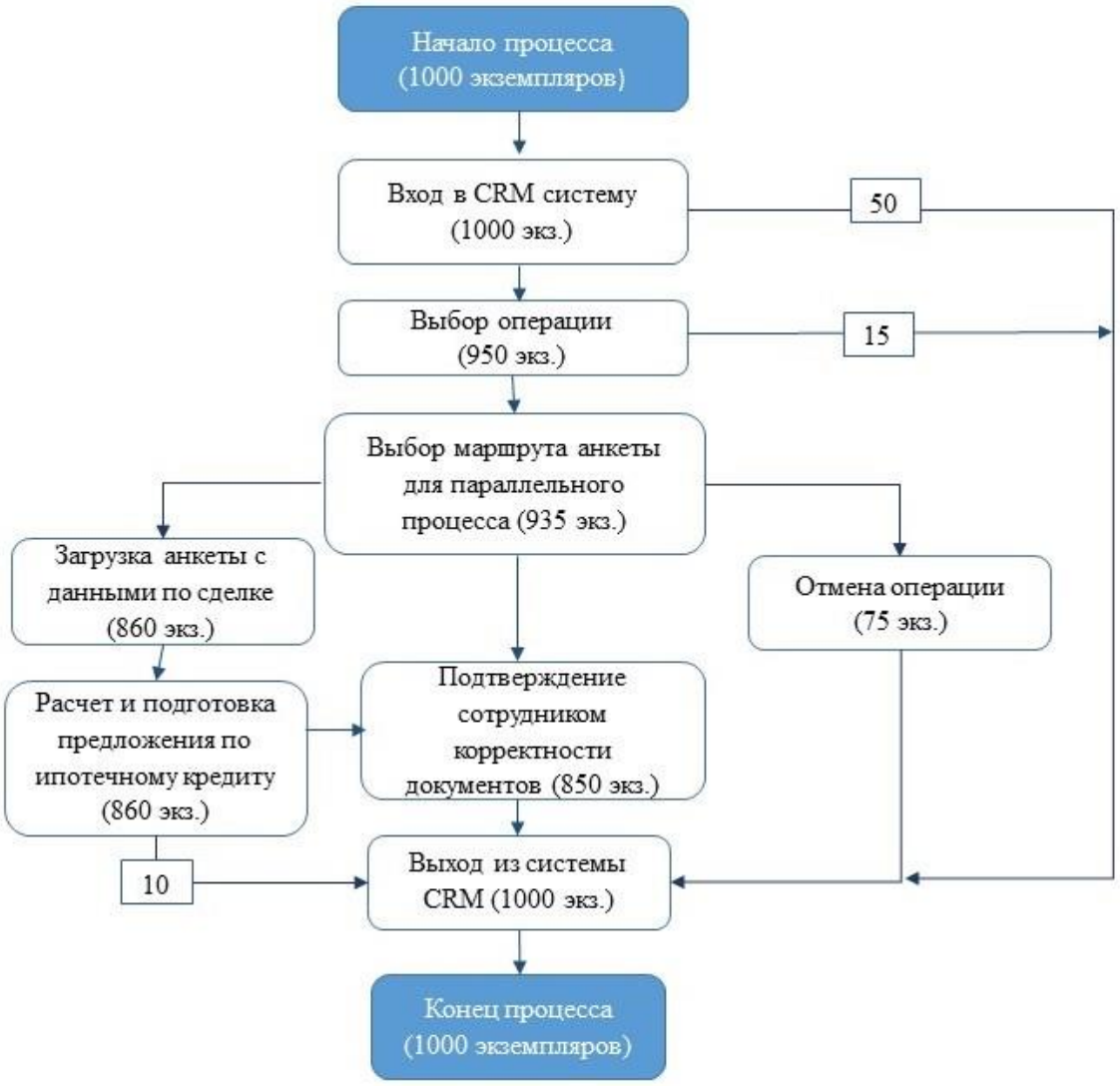

Рисунок 2

Пример метрик представлен в табл. 1:

Таблица 1.

Метрика	**Оформление сделки купли-продажи**	**Выдача ипотечного кредита**
Количество экземпляров процесса в выгрузке	1 000	860
Средняя длительность одной операции	65 мин	80 мин
Вариативность путей процесса (отражает, насколько стандартно исполняется процесс)	97 %	98%
Потери (пустые, незавершенные экземпляры) процесса	140	10
Длительность перехода от одной операции к другой	5 мин	15 мин
Доля повторных операций в общем количестве операций (излишние затраты процесса)	10%	5%

Метрика	Оформление сделки купли-продажи	Выдача ипотечного кредита
Зацикленность переходов: доля повторных переходов в их общем количестве	4%	1%

Таким образом, среди наиболее важных результатов анализа процессов с использованием процессной аналитики могут быть следующие выводы:

- выявлены анкеты клиентов, которые не дошли до шага передачи на параллельный процесс;
- определены шаги процесса, на которых происходит остановка документа и ее причины;
- определены лишние операции в процессе, определены сотрудники, их совершающие, и время, затраченное на эти действия;
- выявлены излишние (повторные проверки) в процессе обработки документов;
- определены причины повторов операций и дана оценка дополнительных затрат времени повторных шагов процесса;
- в результате анализа определены факторы, влияющие на длительность процесса.

3. На **третьем этапе** готовится перечень мероприятий по повышению эффективности процессов с учетом выявленных неоптимальностей и приоритетов, а также устанавливается порядок по регулярному мониторингу контрольных показателей эффективности процесса.

Заключение

Представленный в данный статье упрощенный пример демонстрирует реальные возможности нахождения потенциальных точек для улучшения и оптимизации процессов предприятия с использованием процессной аналитики. Устранение потерь производственной информации и «узких горлышек» процесса может иметь внушительный эффект для организаций с большим количеством связанных массовых процессов.

В современных условиях, когда ценовая конкуренция становится стратегически невыгодным направлением развития компаний, конкурентное преимущество целесообразно искать в повышении эффективности деятельности, снижении ее себестоимости и в повышении скорости взаимодействия с клиентом.

Цифровые экосистемы обладают всеми характеристиками, позволяющими в промышленном масштабе разворачивать инструмент мультипроцессной аналитики, что открывает дополнительные возможности по расширению количества участников (продуктов, сервисов) экосистемы и привлечению большего количества клиентов в периметр взаимодействия.

Литература

1. URL: https://plus.rbc.ru/partners/6265068e7a8aa93ff2d935fc (дата обращения – апрель 2024 г.).
2. URL: https://www.tadviser.ru/a/255928 (дата обращения – апрель 2024 г.).
3. URL: https://www.tf-pm.org /upload / 1590128200840.pdf (дата обращения – апрель 2024 г.).

4. URL: https://hbr.org/2019/04/what-process-mining-is-and-why-companies-should-do-it (дата обращения – апрель 2024 г.).
5. Уманский Р.Ю., Борисов С.Б. Process mining как стратегический инструмент повышения эффективности организации // В книге: Мобильный бизнес: Перспективы развития и реализация систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 52-й международной конференции. – Москва: Национальный институт радио и инфокоммуникационных технологий, 2023. – С. 157-160.
6. URL: https://www.vdaalst.com/ (дата обращения – апрель 2024 г.).
7. URL: https://www.vdaalst.com/publications/p128.pdf (дата обращения – апрель 2024 г.).
8. URL: https://data.tedo.ru/events/process-mining-forum-2022/tedo-pmforum.pdf (дата обращения – апрель 2024 г.).
9. URL: https://pro.rbc.ru/news/5ee70c699a79475983f23d89 (дата обращения –апрель 2024 г.).
10. URL: https://www.celonis.com/process-mining/how-does-process-mining-work/ (дата обращения – апрель 2024 г.).
11. URL: https://www.cnews.ru/news/line/2021-12-09_50_rossijskih_kompanij_planiruet (дата обращения – апрель 2024 г.).
12. URL: https://developers.sber.ru/portal/products/sber-process-mining (дата обращения – апрель 2024 г.).
13. URL: https://processmi.com/terms /multiproczessnaya-analitika/ (дата обращения – апрель 2024 г.).
14. URL: https://processmi.com/blog/multiproczessnaya-analitika-povyshenie-effektivnosti-na-prakticheskih-primerah/ (дата обращения – апрель 2024 г.).
15. URL: https://www.celonis.com/blog/expert-predictions-8-trends-for-process-mining-in-2024-and-beyond/ (дата обращения – апрель 2024 г.).
16. Chapela-Campa D., Dumas M. From process mining to augmented process execution // Software and Systems Modeling, 2023. – № 22. – С. 1977-1986.
17. Уманский Р.Ю. Механизм формирования стратегии развития экосистемы оператора мобильной связи // Инновационная деятельность, 2023. – № 1 (64). – С. 124-136.
18. Нигай Е.А. Формирование цифровых экосистем бизнеса в условиях развития информационного общества: управленческий аспект // Ars Administrandi (Искусство управления), 2023. – Т. 15. – № 3. – С. 353-376.

МОДЕЛЬ ТРАНСФОРМАЦИИ УПРАВЛЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТЬЮ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Н.Л. Кетоева, *к.э.н., доцент, Национальный исследовательский университет «МЭИ», KetoyevaNL@mpei.ru;*
М.А. Знаменская, *к.э.н., Национальный исследовательский университет «МЭИ», ZnamenskayaMA@mpei.ru;*
В.К. Драницына, *Национальный исследовательский университет «МЭИ», KotelnyaVK@mpei.ru.*

УДК 33.332

Аннотация. Статья посвящена актуальным вопросам разработки модели трансформации управления образовательной деятельностью высших учебных

заведений в условиях цифровой экономики. В статье приведен рейтинг цифровой конкурентоспособности стран и проведен анализ проектов и направлений цифровой трансформации отрасли науки и высшего образования Российской Федерации. Исследование показало активное внедрение цифровой трансформации образовательной деятельности высших учебных заведений и необходимость повышения «цифровой зрелости» в них. Основными направлениями развития являются: архитектура цифровой трансформации, развитие цифровых сервисов, управление данными, модернизация инфраструктуры и управление кадровым потенциалом. В процессе исследования выявлена рисковая составляющая «цифровой зрелости». Все вышеперечисленные аспекты предопределили формирование модели. Модель трансформации управления образовательной деятельностью высших учебных заведений в условиях цифровой экономики включает в себя входные и выходные данные, а также создание цифровой образовательной среды с выделенными субъектами и ее оценку. Разработанная модель управления цифровизацией образования в университетах позволит решить проблемы, возникающие на пути к цифровой трансформации образования. Все вышеперечисленное поспособствует формированию «цифрового единства» и «достижению цифровой зрелости», а также сетевому взаимодействию высших учебных заведений по интеграции сервисов и содержанию образования.

Ключевые слова: цифровые проекты; цифровая зрелость; трансформация высшего образования и науки; высшие учебные заведения; цифровая трансформация; цифровое образование; риски; модель трансформации управления образовательной деятельностью.

MODEL OF TRANSFORMATION OF EDUCATIONAL MANAGEMENT IN THE DIGITAL ECONOMY

N.L. Ketoeva, *Ph.D., associate professor, National Research University «Moscow Power Engineering Institute»;*
M.A. Znamenskaya, *Ph.D., National Research University «Moscow Power Engineering Institute»;*
V.K. Dranitsyna, *National Research University «Moscow Power Engineering Institute».*

Annotation. The article is devoted to topical issues of developing a model for transforming the management of educational activities of higher educational institutions in the digital economy. The article provides a rating of the digital competitiveness of countries and analyzes projects and directions for digital transformation of the science and higher education sectors of the Russian Federation. The study showed the active implementation of digital transformation of educational activities of higher education institutions and the need to increase «digital maturity» in them. The main areas of development are: digital transformation architecture, development of digital services, data management, infrastructure modernization and human resources management. During the research, the risk component of «digital maturity» was identified. All of the above aspects predetermined the formation of the model. The model for transforming the management of educational activities of higher educational institutions in the digital economy includes input and output data, as well as the creation of a digital educational environment with dedicated subjects and its evaluation. The developed model for managing the digitalization of education at universities will help solve problems that arise on the way to the digital transformation of education. All of the above will contribute to the formation of «digital unity» and «achieving digital maturity» as well as network interaction between higher educational institutions on the integration of services and

educational content.

Keywords: digital projects; digital maturity; transformation of higher education and science; higher education institutions; digital transformation; digital education; risks; model of transformation of educational management.

Введение

Согласно мировому рейтингу цифровой конкурентоспособности *IMD* (*World Digital Competitiveness Ranking* [4]) в 2021 г. по сравнению с 2020 г. Россия поднялась на первую позицию и заняла 42 место (рис. 1). Лидерами данного рейтинга являются США, Гонконг и Швеция. Одними из основных элементов данного рейтинга являются блоки: «Знания», «Расходы на образование», «Развитие цифровых навыков». Россия пока находится в середине рейтинга и это говорит о необходимости активизации мер по повышению конкурентоспособности страны в области цифровой трансформации.

Ранг 1-32	2020	2021	Изменение	Ранг 33-64	2020	2021	Изменение
США	1	1	-	Чехия	35	33	+2
Гонконг	5	2	+3	Португалия	37	34	+3
Швеция	4	3	+1	Словения	31	35	-4
Дания	3	4	-1	Саудовская Аравия	34	36	-2
Сингапур	2	5	-3	Латвия	38	37	+1
Швейцария	6	6	-	Таиланд	39	38	+1
Нидерланды	7	7	-	Чили	41	39	+2
Тайвань, Китай	11	8	+3	Италия	42	40	+2
Норвегия	9	9	-	Польша	32	41	-9
ОАЭ	14	10	+4	Российская Федерация	43	42	+1
Финляндия	10	11	-1	Кипр	40	43	-3
Республика Корея	8	12	-4	Греция	46	44	+2
Канада	12	13	-1	Венгрия	47	45	+2
Великобритания	13	14	-1	Индия	48	46	+2
Китай	16	15	+1	Словацкая республика	50	47	+3
Австрия	17	16	+1	Турция	44	48	-4
Израиль	19	17	+2	Иордания	53	49	+4
Германия	18	18	-	Румыния	49	50	-1
Ирландия	20	19	+1	Бразилия	51	51	-
Австралия	15	20	-5	Болгария	45	52	-7
Исландия	23	21	+2	Индонезия	56	53	+3
Люксембург	28	22	+6	Украина	58	54	+4
Новая Зеландия	22	23	-1	Хорватия	52	55	-3
Франция	24	24	-	Мексика	54	56	-2
Эстония	21	25	-4	Перу	55	57	-2
Бельгия	25	26	-1	Филиппины	57	58	-1
Малайзия	26	27	-1	Колумбия	61	59	+2
Япония	27	28	-1	Южная Африка	60	60	-
Катар	30	29	+1	Аргентина	59	61	-2
Литва	29	30	-1	Монголия	62	62	-
Испания	33	31	+2	Ботсвана	-	63	Новый
Казахстан	36	32	+4	Венесуэла	63	64	-1

Рисунок 1

Уже сейчас разработана стратегия цифровой трансформации Российской Федерации, куда включены шесть направлений трансформации: здравоохранение, образование, транспорт, развитие городской среды, государственное управление и социальная сфера [1]. Так как наука и образование являются одними из главных составляющих, как рейтинга, так и самой стратегии, рассмотрим их более подробно.

В настоящее время изменения в части высшего образования и науки в Российской Федерации уже претерпели ряд изменений: от «автоматизации» и «цифровизации» до «цифровой трансформации».

Автоматизация – внедрение *IT*-решений, повторяющих имеющиеся процессы.

Цифровизация – улучшение существующих процессов путем внедрения *IT*, учета *Lean*-методов оптимизации процессов, реинжиниринга процессов и анализа данных для принятия решений.

Цифровая трансформация – резкое снижение транзакционных издержек за счет платформ. Соединение возможностей технологий и традиционной сферы деятельности организации приводит к появлению новых продуктов и процессов с принципиально новыми качествами [2, 3].

На данный момент разработаны стратегические ориентиры цифровой трансформации отрасли науки и высшего образования [5], где главной целью является достижение уровня «цифровой зрелости» образовательных организаций высшего образования.

Проблематикой цифровой трансформации образования занимался ряд авторов, в том числе Трофимова Н.Н. [6]. Автором выделены трудности, с которыми сталкиваются образовательные учреждения в процессе цифровой трансформации, рассмотрены преимущества и негативные последствия цифровизации образования. Систематизированы общие критерии, которым должен соответствовать процесс цифровизации образования в условиях экономики знаний. Савельева О.В., Савельев И.В., Данилова А.М., Воронин А.Д. [7] в своей статье проанализировали опрос оценки готовности специалистов к применению цифровых технологий в образовании, а также составлен рейтинг оценки факторов, затрудняющих процесс перехода специалистов к цифровому обучению. Авторы делают вывод о том, что необходимо обеспечить специалистов методической поддержкой в решении вопросов инновационных практик цифровой трансформации, а электронная информационно-образовательная среда вуза является необходимым условием для использования единого открытого образовательного пространства [7]. Бесланеев А.Ж. в рамках своей работы выявил основные проблемы, связанные с внедрением цифровых технологий в управление отраслью образования, основной из которых является проблема трактовки и понимания термина «экономика образования». Одновременно в ходе исследования представлена авторская позиция о трансформации процессов управления в цифровой среде, которая заключается в расширении управленческого поля управляющего субъекта с целью достижения множественных результатов [8], Огоев А.У., Хаблиева С.Р. [9] Авторы посвятили статью цифровой трансформации высшего образования, рассмотрели понятия «информатизация», «цифровизация», «цифровая трансформация образования». Проанализированы основные направления цифровой трансформации высшего образования. Был сделан вывод, что необходимо обновление образовательного процесса в соответствии с новыми требованиями и нормами, техническими условиями, показателями качества и повышение ИКТ-компетентности преподавателей вузов. Мурай О.В. [10] свою статью посвящает цифровой трансформации образования в русле новых

социальных компетенций. Рассматривается цифровая идентификация и социализация, необходимость формирования цифровой компетенции. Дополнительное внимание уделено формированию цифровой идентичности и цифровому самосознанию. Автор выделяет риски введения цифрового образования. Главный риск заключается в том, что вместо индивидуального образования, нацеленного на развитие традиционных и цифровых компетенций, может продолжиться использование стандартных методов обучения, с применением имеющихся у преподавателя под рукой информационно-коммуникационных технологий, эффективность которых остается под вопросом. Шустров А.С., Смертин И.В., Земнухов Е.С. исследуя различные вопросы, связанные с процессом цифровой трансформации образования выявили, что в настоящее время большинство работников образовательных организаций активно используют в своей профессиональной деятельности возможности информационно-коммуникационных технологий, осознавая перспективы развития цифровизации образования в современном обществе, необходимость обновления подходов к организации образовательного процесса и повышения его качества [11], Щучка Т.А. в своей статье ставит проблему реализации цифровой трансформации образования и предпринимает попытку ее решения. Автором сделан вывод, что именно педагогическая составляющая должна определять содержательную сторону дидактического цифрового поля и ее результативность в отношении методик и методологий цифровых обучающих программ, активно разрабатываемых учеными в последние годы [12].

В связи с проведенным анализом, можно сказать, что процесс цифровой трансформации образовательной деятельности уже внедряется в стране. Этот процесс затрагивает как государственные структуры и органы, высшие учебные заведения, так и преподавателей, обучающихся и родителей. Ключевыми направлениями цифровой трансформации образовательной организации высшего образования являются: цифровые сервисы, информационные системы, инфраструктура, управление данными и кадры.

Таким образом, основными проблемами исследования является анализ и выявление путей и способов трансформации управления образовательной деятельностью высших учебных заведений в условиях цифровой экономики.

Исследование включает в себя следующие разделы: введение, материалы и методы, результаты, обсуждение, заключение и список использованной литературы.

Научная новизна исследования заключается в разработке модели трансформации управления образовательной деятельностью университетов в условиях цифровой экономики, отличительной особенностью которой является учет инновационных рисков, связанных с реализуемыми инновационными проектами, а также оценкой уровня цифровой трансформации образовательной деятельности по разработанной авторами методике.

Исходя из этого, цель исследования заключается в разработке модели трансформации управления образовательной деятельностью университетов в условиях цифровой экономики, учитывающая рисковую составляющую реализуемых инновационных проектов в университетах.

Для достижения данной цели были поставлены и решены следующие задачи:

- проанализирован рейтинг цифровой конкурентоспособности стран;
- проанализированы направления и проекты на пути к цифровой трансформации образовательной деятельности;
- разработана модель трансформации управления образовательной деятельностью высших учебных заведений.

Объектом исследования выступает цифровая трансформация образовательной деятельности Российской Федерации.

Предметом исследования является модель трансформации управления образовательной деятельностью университетов в условиях цифровой экономики Российской Федерации.

Методологический аппарат составили следующие методы исследования: диалектического научного познания и частные научные (анализ, синтез, сравнение, логический и системно-структурный анализ, формализация, анализ нормативно-правовых документов), моделирование.

При изучении отрасли науки и высшего образования с точки зрения их цифровой трансформации были изучены цифровые проекты и треки образовательной деятельности.

Стратегия цифровой трансформации отрасли науки и высшего образования России предполагает работы по пяти направлениям (трекам) цифровой трансформации (рис. 2). Все направления работ являются важными для российских высших учебных заведений и требуют глубокой проработки [13].

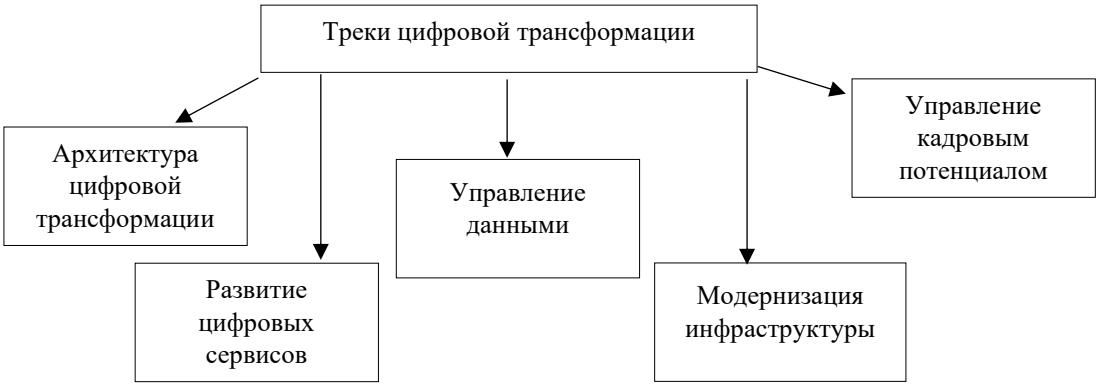

Рисунок 2

В рамках представленной стратегии цифровой трансформации [5] разработаны долгосрочные цели реализации стратегии цифровой трансформации (табл. 1).

Таблица 1.

№	Направление (треки)	Долгосрочные цели
1	Архитектура цифровой трансформации	• Разработана и реализована стратегия цифровой трансформации. • Разработана и внедрена *BI*-система, позволяющая в режиме реального времени мониторить процесс цифровой трансформации сферы науки и высшего образования.
2	Развитие цифровых сервисов	• Все значимые услуги университета доступны в электронном виде. • Создание единой информационной среды взаимодействия общества, бизнеса, науки и образования.
3	Управление данными	• Функционирует система поддержки принятия управленческих решений, принимающая данные в формате стриминга. • Система настроена на формирование

№	Направление (треки)	Долгосрочные цели
		предиктивной аналитики.
4	Модернизация инфраструктуры	• 100% замена морально устаревшего оборудования, использующегося для образовательного процесса. • Инфраструктура, отвечающая современным техническим требованиям.
5	Управление кадровым потенциалом	• В университете работают команды цифровой трансформации. • 100% ППС и АУП в университете обладают цифровыми компетенциями.

Кроме этого, стратегия цифровой трансформации отрасли науки и высшего образования России включает семь проектов [13], каждый из которых должен обеспечить продвижение к «цифровой зрелости» по одному или сразу по нескольким из пяти названных выше направлений (табл. 2).

Таблица 2.

№	Проекты	Сущность
1	Датахаб	Обеспечение доступа бизнеса к результатам исследований высших учебных заведений и сервисы для граждан на основе этих данных.
2	Архитектура цифровой трансформации	*BI*-система для сопровождения организаций в процессе их цифровой трансформации, отслеживающая их «цифровую зрелость».
3	Цифровой университет	Это сервис, охватывающий не только онлайн-занятия и управление расписанием, но и мониторинг научной активности, кадровые, финансовые и другие административные процессы.
4	Единая сервисная платформа науки	Единая экосистема сервисов и услуг для ученых для совместных исследований, а также доступа к международным базам данных и существующим мерам поддержки
5	Маркетплейс программного обеспечения и оборудования	Единая информационная среда для взаимодействия высших учебных заведений и поставщиков оборудования и программного обеспечения
6	Цифровое образование	Развитие цифровых компетенций как у студентов, так и у научно-педагогических работников
7	Сервис хаб	Систематизация и регламентирование бизнес-процессов в высших учебных заведениях и в Министерстве науки и высшего образования с помощью отдельной разработанной информационной системы

Таким образом, высшие учебные заведения ожидает «цифровое единство» и «достижение цифровой зрелости». К 2030 г. все описанные выше сервисы будут взаимосвязаны между собой, а это требует разработки новой модели трансформации управления образовательной деятельностью высших учебных заведений (рис. 3).

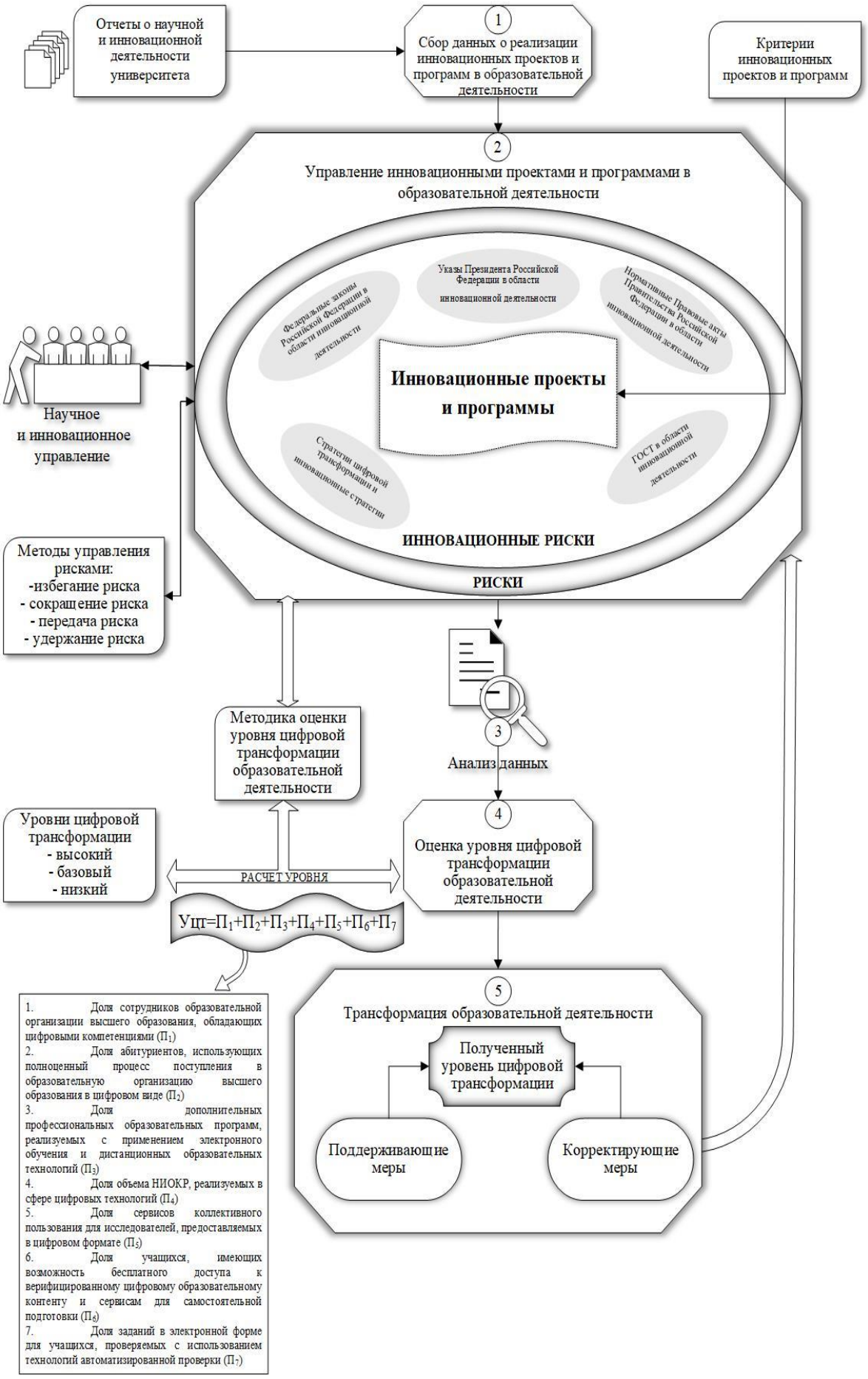
Отчеты о научной и инновационной деятельности университета
1
Сбор данных о реализации инновационных проектов и программ в образовательной деятельности
Критерии инновационных проектов и программ
2
Управление инновационными проектами и программами в образовательной деятельности
Федеральные законы Российской Федерации в области инновационной деятельности
Указы Президента Российской Федерации в области инновационной деятельности
Нормативные Правовые акты Правительства Российской Федерации в области инновационной деятельности
Инновационные проекты и программы
Стратегии цифровой трансформации и инновационные стратегии
ГОСТ в области инновационной деятельности
ИННОВАЦИОННЫЕ РИСКИ
РИСКИ
Научное и инновационное управление
Методы управления рисками:
-избегание риска
- сокращение риска
- передача риска
- удержание риска
Методика оценки уровня цифровой трансформации образовательной деятельности
3
Анализ данных
Уровни цифровой трансформации
- высокий
- базовый
- низкий
РАСЧЕТ УРОВНЯ
4
Оценка уровня цифровой трансформации образовательной деятельности
Уцт=П1+П2+П3+П4+П5+П6+П7
1. Доля сотрудников образовательной организации высшего образования, обладающих цифровыми компетенциями (П1)
2. Доля абитуриентов, использующих полноценный процесс поступления в образовательную организацию высшего образования в цифровом виде (П2)
3. Доля дополнительных профессиональных образовательных программ, реализуемых с применением электронного обучения и дистанционных образовательных технологий (П3)
4. Доля объема НИОКР, реализуемых в сфере цифровых технологий (П4)
5. Доля сервисов коллективного пользования для исследователей, предоставляемых в цифровом формате (П5)
6. Доля учащихся, имеющих возможность бесплатного доступа к верифицированному цифровому образовательному контенту и сервисам для самостоятельной подготовки (П6)
7. Доля заданий в электронной форме для учащихся, проверяемых с использованием технологий автоматизированной проверки (П7)
5
Трансформация образовательной деятельности
Полученный уровень цифровой трансформации
Поддерживающие меры
Корректирующие меры

Рисунок 3

Данная модель отличается от существующих разработок тем, что она учитывает инновационные риски, связанные с инновационными проектами, которые реализуются в университетах, а также оценивает уровень цифровой трансформации образовательной деятельности по разработанной авторами формуле.

Критериями инновационных проектов выступают:

1. *Новаторство.* Инновационный проект должен представлять новое решение, которого не существовало ранее. Новизна может касаться продукта, процесса или услуги. Новизна должна подкрепляться наличием результата интеллектуальной деятельности, которое может выражаться в виде патента, изобретения, полезные модели, средства для ЭВМ, базы данных и т.п.

2. *Рискованность.* В связи с неопределенностью результатов, инновационные проекты могут быть связаны с некоторыми рисками и неопределенностью. Команда проекта должна уметь управлять рисками и оперативно реагировать на возникшие проблемы.

3. *Открытость для изменений.* Инновационный проект не может быть жестко закрепленным на начальном этапе, так как в процессе реализации могут измениться условия или потребности пользователей. Команда проекта должна быть готова к изменениям и гибко реагировать на новые требования.

4. *Перспективность.* Инновационный проект должен иметь потенциал для долгосрочной успешной реализации и привлечения новых инвесторов. Это означает, что он должен решать актуальные проблемы и быть конкурентоспособным на рынке.

Первым этапом в модели производится сбор данных о реализации инновационных проектов и программ в образовательной деятельности. Для этого изучаются отчеты о научной и инновационной деятельности университета. Ответственным подразделением за выполнение данного этапа является научное и инновационное управление университетов.

Второй этап – это управление инновационными проектами и программами. Все инновационные проекты и программы должны выполняться в соответствии с нормативно-правовыми документами. Среди них Указы Президента Российской Федерации, Федеральные законы Российской Федерации в области инновационной деятельности, Нормативные Правовые акты Правительства Российской Федерации в области инновационной деятельности, ГОСТ в области инновационной деятельности, Стратегии цифровой трансформации и инновационные стратегии [14]. В табл. 3 представлена нормативно-правовая база инновационной деятельности.

Таблица 3.

Нормативная правовая база инновационной деятельности	**Название**
Законы Российской Федерации	Федеральный закон РФ от 23.08.1996 № 127-ФЗ «О науке и государственной научно-технической политике».
	Федеральный закон РФ от 31.12.2014 № 488-ФЗ «О промышленной политике в Российской Федерации».
Указы Президента Российской Федерации	Указ Президента РФ от 07.07.2011 N 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации».

Нормативная правовая база инновационной деятельности	Название
	Указ Президента РФ от 01.12.2016 N 642 «О Стратегии научно-технологического развития Российской Федерации».
Нормативные правовые акты Правительства Российской Федерации	Постановление Правительства РФ от 09.04.2010 № 218 «О мерах государственной поддержки развития кооперации российских высших учебных заведений, государственных научных учреждений и организаций, реализующих комплексные проекты по созданию высокотехнологичного производства».
	Постановление Правительства РФ от 09.04.2010 № 219 «О государственной поддержке развития инновационной инфраструктуры в федеральных образовательных учреждениях высшего профессионального образования».
	Постановление Правительства РФ от 09.04.2010 № 220 «О мерах по привлечению ведущих ученых в российские образовательные учреждения высшего профессионального образования».
	Постановление Правительства РФ от 15.04.2014 № 316 «Об утверждении государственной программы Российской Федерации «Экономическое развитие и инновационная экономика».
	Постановление Правительства РФ от 29.03.2019 № 377 «Об утверждении государственной программы Российской Федерации «Научно-технологическое развитие Российской Федерации».
	Постановление Правительства РФ от 01.08.2020 № 1156 «Об утверждении Правил предоставления грантов в форме субсидий из федерального бюджета на реализацию проектов по созданию и развитию инжиниринговых центров на базе образовательных организаций высшего образования и научных организаций».
Стратегии цифровой трансформации и инновационные стратегии	Стратегии цифровой трансформации регионов России.
	Стратегия цифровой трансформации образования.
	Стратегия цифровой трансформации отрасли науки и высшего образования.
	Стратегия инновационного развития Российской Федерации.
	Стратегия научно-технологического развития Российской Федерации.
ГОСТ	ГОСТ Р 59871-2021 Информационно-коммуникационные технологии в образовании. Цифровая научно-образовательная среда.
	ГОСТ Р 59870-2021 Информационно-коммуникационные технологии в образовании. Цифровой университет.
	ГОСТ Р ИСО 56000-2021 Инновационный менеджмент.
	ГОСТ Р 56261-2014 Инновационный менеджмент. Инновации.

В процессе управления инновационными проектами устанавливаются цель и задачи проекта, а также план выполнения проекта, то есть установления целевых показателей на определенные временные промежутки времени. Далее рассматриваются инновационные проекты и программы, реализуемые в университете. Для каждого проекта или программы существуют свои критерии. Например, для проекта Приоритет-2030 – это технологическое (инновационное) предпринимательство в университете; портфель патентов университета; сотрудничество университета с высокотехнологичными компаниями; проводимые университетом испытания; инновационная инфраструктура университета, предприятия университета, социальное предпринимательство; НИОКР университета; базовые кафедры университета [15]. Для программы цифровой трансформации образовательной организации высшего образования показателями выступают системы управления на основе данных (доля расходов на ИТ от общих расходов образовательной организации высшего образования; доля цифровых сервисов, доступных пользователям в единой цифровой среде от общего числа сервисов, предоставляемых образовательной организацией высшего образования; доля ключевых субъектов образовательной организации высшего образования, для которых построены цифровые инструменты обратной связи и проактивного управления на основе анализа данных); цифровые образовательные технологии (количество студентов других образовательных организаций высшего образования, использующих цифровые образовательные ресурсы, разработанные образовательной организацией высшего образования (виртуальные лаборатории, адаптивные курсы, обучающие материалы с использованием технологий виртуальной реальности, тренажеры, симуляторы); доля цифрового образовательного контента образовательной организации высшего образования, доступного учащемуся в единой цифровой среде; доля образовательных программ, использующих внешние онлайн-курсы по выбору учащихся (МООК, курсы университетов-партнеров, и др.); доля онлайн-курсов, с численностью обучающихся не менее 5000 человек, размещенных на зарубежных открытых образовательных платформах (*Coursera, EdX, FutureLearn*); количество онлайн-курсов, размещенных на открытых образовательных платформах, с численностью обучающихся не менее 5000 человек); индивидуальные образовательные траектории (среднее количество студентов на уникальной образовательной траектории – рассчитывается как общее количество студентов образовательной организации высшего образования, поделенное на количество уникальных образовательных траекторий (набор курсов/дисциплин/модулей, которые студент изучает за все время нахождения в образовательной организации высшего образования). Рассчитывается на основании фактического количества студентов и фактических траекторий студентов (курсы/дисциплины/модули, которые студенты выбрали): доля обучающихся с уникальной индивидуальной образовательной траекторией; доля обучающихся, которые используют индивидуализированные сервисы навигации по образовательному пространству (рекомендательная система, основанная на анализе «цифрового следа» и инструментах диагностики с применением искусственного интеллекта); компетенции цифровой экономики (доля образовательных программ образовательного учреждения, в которые включено освоение цифровых компетенций) [16].

Также на этом этапе учитываются риски, возникающие в процессе выполнения инновационного проекта, а именно инновационные риски, представленные в табл. 4. Ответственное подразделение проводит анализ рисков и осуществляет управление ими по четырем основным методам: избегание риска, сокращение риска, передача риска, удержание риска.

Таблица 4.

Группа	Риск
Правовые	Нарушение авторских прав третьих лиц в ходе работы над проектом
Экономические	Недостаточное количество инвестиционных и финансовых ресурсов для успешного осуществления проекта, вследствие чего возникают простои и отставание от графика выполнения этапов проекта
	Изменение спроса со стороны заказчиков на инновации, что в свою очередь приводит к невозможности реализации нового изделия на рынке
Организационные	Утечка стратегически важной для успешной реализации проекта информации на сторону из-за нарушения коммерческой тайны
	Отставание от запланированных сроков в части проведения НИОКР
Научно-технические	Неадекватность коммерческого результата от реализации новой продукции из-за ошибочного выбора инновационного проекта
	Недостаточная обеспеченность проекта необходимыми ресурсами, что в конечном итоге приводит к отклонению фактических показателей проекта от планируемых

Ответственным подразделением, занимающимся управлением инновационными проектами и программами в образовательной деятельности, является научное и инновационное управление.

Данный отдел занимается выполнением следующих задач:

- координирование деятельности структурных подразделений университета в части развития научно-исследовательской деятельности, а также инноваций;
- организационно-методической поддержкой разработки и реализации научно-исследовательских и инновационных проектов структурных подразделений университета;
- развитие научного и научно-технического сотрудничества с вузами, научными, проектно-конструкторскими организациями, предприятиями и фирмами, зарубежными партнерами в целях усиления интеграционных процессов образования, науки и промышленности, повышения эффективности научной и инновационной деятельности;
- создание условий для защиты интеллектуальной собственности и авторских прав исследователей и разработчиков для выхода научных коллективов университета на мировой рынок высокотехнологичной продукции.

Далее анализируются полученные данные и проводится оценка уровня цифровой трансформации (Уцт) образовательной деятельности по разработанной авторами методике. Ответственным на этом этапе также является научное и инновационное управление.

Данная методика включает в себя семь показателей:

1. Доля сотрудников образовательной организации высшего образования, обладающих цифровыми компетенциями ($П_1$).

2. Доля абитуриентов, использующих полноценный процесс поступления в образовательную организацию высшего образования в цифровом виде ($П_2$).

3. Доля дополнительных профессиональных образовательных программ,

реализуемых с применением электронного обучения и дистанционных образовательных технологий ($П_3$).

4. Доля объема НИОКР, реализуемых в сфере цифровых технологий ($П_4$).

5. Доля сервисов коллективного пользования для исследователей, предоставляемых в цифровом формате ($П_5$).

6. Доля учащихся, имеющих возможность бесплатного доступа к верифицированному цифровому образовательному контенту и сервисам для самостоятельной подготовки ($П_6$).

7. Доля заданий в электронной форме для учащихся, проверяемых с использованием технологий автоматизированной проверки ($П_7$).

Формула оценки уровня цифровой трансформации имеет следующий вид:

$$Уцт = П_1+П_2+П_3+П_4+П_5+П_6+П_7$$

Каждый показатель оценивается от 0 до 1 балла методом ранжирования (экспертные оценки). Далее путем суммирования получается итоговый балл, который показывает уровень цифровой трансформации образовательной деятельности университета

Цифровая трансформация образовательной деятельности делится на три уровня, представленные в табл. 5.

Таблица 5.

Уровень	**Баллы**
Высокий	$6 \leq Уцт \leq 7$
Базовый	$4 \leq Уцт < 6$
Низкий	$0 \leq Уцт < 4$

Следующим этапом, исходя из полученного уровня цифровой трансформации образовательной деятельности, применяются корректирующие меры, если уровень ниже высокого, или поддерживающие меры – для удержания результата, если уровень является высоким. Как и в предыдущих этапах, ответственным за выполнение данного этапа выступает научное и инновационное управление.

Поддерживающими мерами могут быть:

- увеличение целевых показателей с целью дать мотивацию к достижению наилучшего результата;
- развитие команды проекта, то есть повышение квалификации участников проекта;
- учет мнений участников проекта, то есть сбор отзывов и предложений и т.д.

Корректирующими мерами могут быть:

- корректировка поставленных задач и целевых показателей;
- пересмотр плана проекта;
- привлечение дополнительного финансирования на выполнение проекта;
- привлечение дополнительных человеческих ресурсов;
- усиление контроля за своевременным и четким распределением необходимой информации между участниками проекта и т.д.

После примененных мер снова идет возврат к блоку управление инновационными проектами и программами в образовательной деятельности.

Далее проводятся заново анализ и оценка уровня цифровой трансформации образовательной деятельности, проводится сравнение нового результата с предыдущим, делаются выводы. Данный процесс повторяется до конца реализации инновационного проекта.

В работе Н.В. Ломоносовой и О.П. Осиповой на тему «Мониторинг уровня цифровой трансформации образования: показатели и технологии» рассмотрены основные вопросы мониторинга цифровой трансформации общего образования с учетом оценки степени интеграции сквозных цифровых технологий [17]. На основании данных аспектов в статье разработана модель трансформации управления образовательной деятельностью в условиях цифровой экономики, отличающаяся от существующих разработок тем, что она учитывает инновационные риски, связанные с инновационными проектами, которые реализуются в университетах, а также оценивает уровень цифровой трансформации образовательной деятельности по разработанной авторами формуле. Данная модель ориентирована на высшее образование.

Авторами рассмотрены инновационные риски проекта. Схожее мнение по поводу инновационных рисков просматривается в работе автора Р.В. Приходько «Инновационные риски: содержание и способы их предотвращения» [18]. Авторами проведена классификация этих рисков по четырем группам.

Авторами также были включены в модель методы управления рисками. С основными методами, которые выделены в учебном пособии М.И. Раскатовой «Теоретические основы управления рисками», авторы согласны и используют их в своем исследовании [19].

Заключение

Цифровая образовательная среда является совокупностью информационных систем, источников, инструментов, содержащих в себе новые технологии получения образования в интерактивной форме, которая не только интересна, но и полезна, так как увеличивает вовлеченность студентов к получению знаний, а не диплома об образовании.

В работе приведена разработка модели трансформации управления образовательной деятельностью в условиях цифровой экономики, которая учитывает инновационные риски инновационного проекта и оценивает уровень цифровой трансформации образовательной деятельности. Данная модель может быть внедрена в образовательную организацию высшего образования, что позволит оценить эффективность данной разработки, как в экономическом, так и в социальном плане.

Литература

1. Стратегия цифровой трансформации Российской Федерации.
2. Потаповой Е.Г., Потеева П.М., Шклярук М.С. Стратегия цифровой трансформации: написать, чтобы выполнить / под ред. Е.Г. Потаповой. – М.: РАНХиГС, 2021. – 184 с.
3. Сьюзан Граджек. Вице-президент EDUCAUSE «Цифровая трансформация высшего образования».
4. Сайт IMD World Digital Competitiveness Ranking https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/
5. Распоряжение Правительства РФ от 21.12.2021 г. n 3759-р «Стратегическое направление в области цифровой трансформации науки и высшего образования».
6. Трофимова Н.Н. Влияние цифровизации на образование в условиях экономики

знаний // Экономика образования, 2023. – № 3. – С. 93-102.
7. Савельева О.В., Савельев И.В., Данилова А.М., Воронин А.Д. Цифровая трансформация: оценка готовности специалистов к применению цифровых технологий в образовании // Ученые записки университета им. П.Ф. Лесгафта, 2023. – № 3. – С. 400-404.
8. Бесланеев А.Ж. Цифровые технологии в управлении образованием: основные проблемы цифровизации отрасли, перспективные проекты и наработки //Инновации и инвестиции, 2023. – № 3. – С. 164-170.
9. Огоев А.У., Хаблиева С.Р. Цифровая трансформация образования: перспективы и новые возможности // Вестник Северо-Осетинского государственного университета имени К.Л. Хетагурова, 2023. – № 1. – С. 117-123.
10. Мурай О.В. Цифровизация информации как вызов современной образовательной системе // Педагогический журнал, 2023. – № 1-1. – С. 427-433.
11. Шустров А.С., Смертин И.В., Земнухов Е.С. Цифровая трансформация образования: ключевые проблемы и пути их решения // Психолого-педагогический поиск, 2023. – № 1. – С. 71-78.
12. Щучка Т.А. Цифровая трансформация образования в контексте анализа программных средств//Современный ученый, 2023. – № 2. – С. 241-245.
13. Сайт Skillbox Образование 4.0 https://skillbox.ru/media/education/opublikovana-strategiya-tsifrovoy-transformatsii-nauki/?ysclid=lkhogc4sbg23293298
14. Официальный сайт Министерства экономического развития и промышленности Ульяновской области https://ekonom73.ru/mesmerize/activities/departament-investitsionnoj-politiki/otdel-razvitiya-innovatsij-i-predprinimatelskoj-deyatelnosti/innovatsionnaya-deyatelnost/normativnaya-pravovaya-baza-innovatsionnoj-deyatelnosti/ (дата обращения 10.08.2023).
15. Национальный рейтинг университетов. URL: https://academia.interfax.ru/ru/ratings/?page=1&rati ng=1&year=2022 (дата обращения: 10.08.2023).
16. Постановление Правительства РФ от 3 мая 2019 г. N 552 «Об утверждении Правил предоставления грантов в форме субсидий из федерального бюджета некоммерческим организациям на реализацию отдельных мероприятий федерального проекта «Кадры для цифровой экономики» национальной программы «Цифровая экономика Российской Федерации».
17. Ломоносова Н.В., Осипова О.П. Трансформация системы управления образовательным процессом в высшем образовании в условиях цифровизации // Преподаватель XXI век. 2021. – № 4-1. URL: https://cyberleninka.ru/article/n/transformatsiya-sistemy-upravleniya-obrazovatelnym-protsessom-v-vysshem-obrazovanii-v-usloviyah-tsifrovizatsii (дата обращения: 13.08.2023).
18. Приходько Р.В. Инновационные риски: содержание и способы предотвращения // Экономика и экологический менеджмент, 2022. – № 2. URL: https://cyberleninka.ru/article/n/innovatsionnye-riski-soderzhanie-i-sposoby-predotvrascheniya (дата обращения: 13.08.2023).
19. Раскатова М.И. Теоретические основы управления рисками: учебное пособие. – Челябинск: Издательский центр ЮУрГУ, 2019. – 46 с.

ЦИКЛИЧНОСТЬ В ЭКОНОМИКЕ: ТЕОРИИ, ПРИЧИНЫ И СПЕЦИФИКА ПРОЯВЛЕНИЯ В РОССИЙСКОЙ ЭКОНОМИКЕ

В.Д. Зюзин, *Нижегородский государственный университет им. Лобачевского, v.d.zyuzin@gmail.com;*
Н.А. Башмуров, *Нижегородский государственный университет им. Лобачевского, bashmurov.nikolai@yandex.ru;*
М.Д. Зюзина, *Вознесенская СОШ, mariazyu@mail.ru.*

УДК 338.2:330.101.541(470)

Аннотация. В данной статье рассматривается актуальная тема цикличности экономического развития и ее влияния на общее благосостояние общества. Исследование начинается с обзора истории экономической мысли о цикличности, начиная с 19 века и заканчивая современными теориями. Авторы анализируют различные аспекты экономических циклов, включая их классификацию, фазы, причины и специфику проявления в российской экономике, а также рассматривают последствия кризиса 2022 г. В работе делается акцент на отсутствии теоретического единства в понимании экономических циклов, что делает ее особенно значимой для современной экономической науки. Исследование основывается на анализе макроэкономических данных, исторических событий и теорий цикличности, предложенных известными экономистами. Целью статьи является глубокое понимание механизмов цикличности и выявление путей минимизации негативных последствий экономических спадов для российской экономики.

Ключевые слова: цикличность; экономические циклы; российская экономика; кризис 2022 г; макроэкономика; теории экономического роста.

CYCLICALITY IN ECONOMY: THEORIES, CAUSES, AND SPECIFICS OF MANIFESTATION IN THE RUSSIAN ECONOMY

Vladislav Zyuzin, *Nizhny Novgorod State University Lobachevsky;*
Nikolay Bashmurov, *Nizhny Novgorod State University named after N.Y. Lobachevsky;*
Mariya Zyuzina, *Voznesenskaya Secondary School.*

Annotation. This scientific paper examines the pertinent topic of economic cyclicality and its impact on the overall well-being of society. The study begins with a review of the history of economic thought on cyclicality, starting from the 19th century and ending with contemporary theories. The authors analyze various aspects of economic cycles, including their classification, phases, causes, and the specifics of their manifestation in the Russian economy, as well as considering the consequences of the 2022 crisis. The work emphasizes the absence of theoretical unity in understanding economic cycles, making it particularly significant for modern economic science. The research is based on the analysis of macroeconomic data, historical events, and theories of cyclicality proposed by renowned economists. The article aims to deeply understand the mechanisms of cyclicality and identify ways to minimize the negative consequences of economic downturns for the Russian economy.

Keywords: cyclicality; economic cycles; Russian economy; 2022 crisis; macroeconomics; economic growth theories.

Актуальность исследования

Человечество постоянно ищет возможности и решения для улучшения собственного благосостояния и уровня жизни, что предопределяется экономическим ростом. Тем не менее рост не может осуществляться постоянно, существуют падения и экономическая нестабильность.

Если рассматривать экономику за последние несколько столетий, то можно найти огромное число примеров неустойчивости рыночной экономики. Всегда вслед за периодом роста и развития, обеспечения экономического успеха возникает период спада и рецессии, которые совмещены с такими понятиями, как падение объема производства и рост безработицы. Также рассмотрение экономики в динамике показывает, что все это имеет циклическую последовательность, а каждый новый уровень предопределяется новым научно-техническим прорывом, толчком.

Данная тема соотносится с одним из наиболее сложных разделов макроэкономики. Это связано с отсутствием теоретического единства, так как имеется существенное количество методик и подходов, включая применение математического аппарата.

Первые попытки объяснить экономические основы роста были предприняты еще в начале 19 века. Именно тогда экономисты заметили циклы с их падениями и подъемами. Представленная проблема обрела мировое значение, поэтому можно найти существенное количество работ по заданной тематике. Циклическое развитие изучали экономисты Туган-Барановский, К. Маркс, Кейнс, Кондратьев и многие другие [1].

Большинство авторских теорий соотносится с понятием неопределенности, поэтому при их описании часто использовались выражения «вероятно», «возможно» и так далее.

Авторы труда «Макроэкономика. Глобальный подход» указывали на тот факт, что на текущий момент до сих пор не существует ни одной экономической теории, которая подтверждена и отличается единством подхода для каждого специалиста. Это является существенной проблемой, поставленной перед современниками.

Цель научной статьи предполагает изучение и раскрытие ключевых проблем цикличности развития экономики. Для ее достижения необходимо решить ряд задач:

- Описать характеристики экономических циклов на современном этапе.
- Рассмотреть понятие о цикличности в экономике, классификацию экономических циклов.
- Изучить фазы экономического цикла.
- Определить причины цикличности экономического развития.
- Выявить проблемы цикличности в российской экономике.
- Изучить причины кризиса 2022 г.

Понятие о цикличности в экономике, классификация экономических циклов

Понятие «цикл» пошло из греческого языка и переводилось как «круг». В современности под этим определением следует понимать совокупность связанных между собой явлений, процессов, работ и других экономических элементов, которые проходят по кругу в течение отдельного периода времени [2].

Под цикличностью следует понимать норму движения развития экономики, которая сопровождается различными колебаниями и неравномерностями, спадами и подъемами. Именно цикличность относят к одному из способов обеспечения

саморегуляции рыночной экономики. Стоит отметить, что цикличность сопровождается существенной чувствительностью к государственным рычагам управления, влияющим на социально-экономические процессы [2].

Под экономическим циклом следует понимать период времени, во время которого происходит как спад, так и подъем экономической активности (изменение уровня производства, занятости на рынке труда, цен и прочих показателей) [2].

Наличие цикличности практически никак не влияет на долгосрочный тренд экономического развития. Это означает, что в будущем общая динамика деловой активности будет повышаться даже в момент спада или вхождения в депрессию. Представленную особенность можно выразить графически на рис. 1 (экономический цикл [2]), где циклические колебания представлены в виде волны, а трендовое направление – пунктиром.

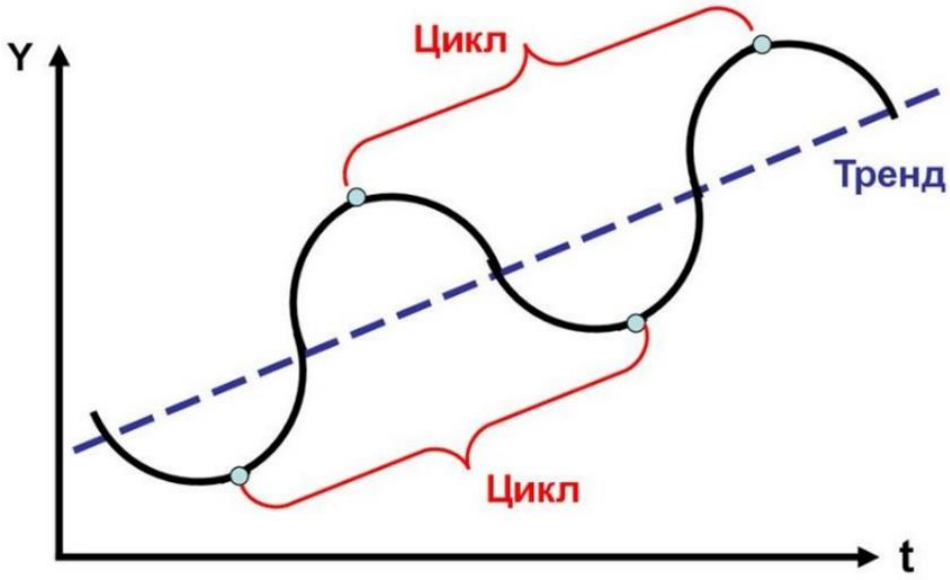

Рисунок 1

На текущий момент в библиографических источниках существует более 1380 типов цикличности экономики. Что касается классификации, то здесь можно выделить следующие [8, с. 19]:

По сфере применения:

- аграрные;
- промышленные.

По особенностям проявления:

- нефтяные;
- продовольственные;
- энергетические;
- сырьевые;
- экологические;
- валютные и другие.

По признаку территориальной принадлежности:

- национальные;
- наднациональные;
- международного уровня.

По особенности развертывания:

- структурные;
- отраслевые.

Еще одна важная классификация циклов связывается с продолжительностью их протекания. В современной практике существуют четыре основных категории и две дополнительные с расширенной продолжительностью [3]:

- Цикл Китчина (протекает в течение 2-4 лет).
- Цикл Жюгляра (среднесрочное протекание за 8-10 лет).
- Ритм Кузнеца (долгосрочный цикл с продолжительностью 15-25 лет).
- Волны Кондратьева (цикличность проявляется в периоде 45-55 лет).
- Циклы Форрестера (оценивание экономических циклов на промежутке 200 лет).
- Циклы Тоффлера (цикличность экономики в промежутке 1000-2000 лет).

Первая разновидность циклов получила название в честь ученого Дж. Китчина. Последний посвятил собственное исследование изменениям на потребительском рынке. Согласно полученным данным в течение 2-4 лет протекают события, связанные с нарушением и восстановлением равновесия в определенной точке спроса и предложения. Эти циклы часто соотносятся с вводом новых средств труда и с вливанием новых инвестиций.

Многие современные экономисты, которые разделяют представленную теорию, рассматривают краткосрочные экономические циклы в разрезе среднесрочных. Над последними плотного работал К. Жюгляр, который посвятил собственные труды макроэкономической нестабильности. Большинство проблем развития экономики зачастую связывалось с проводимой политикой правительства.

Среднесрочный цикл получил и другие названия, включая «промышленный», «деловой», «классический». Кризис в Англии в начале 1825 г. стал ярким примером такого цикла. Ключевая причина спадов и роста экономики связывалась с потребностью обновления основного капитала. В модели К. Жюгляра четко прослеживаются колебания в ВВП, инфляции, на рынке труда и т.д. [4].

С течением времени начали появляться и долгосрочные методики определения экономических циклов. Практически идеальную модель предложил Саймон Кузнец, уроженец современной Республики Беларусь. Ученый и практик смог объединить труды Китчина и Жюгляра в более длительной перспективе. Обычно циклы Кузнеца рассматриваются в течении 15-25 лет, а цикличность базируется на обновлении основных фондов, использовании новых технологий и так далее [3].

Развитием теорией циклов занимался российский ученый Кондратьев. Он предложил определять экономические циклы на отрезке 45-55 лет. По мнению теоретика, наиболее сильные кризисы происходят в момент наложения долгосрочного цикла на среднесрочный. Примером подобного состояния считается «Великая Депрессия».

Стоит обратить внимание, что более продолжительные типы циклов используются реже. Они часто соотносятся с крупными социально-экономическими событиями, трансформацией одного управленческого строя в другой.

Фазы экономического цикла

Экономический цикл можно разделить на следующие характерные фазы: Кризис (рецессия, спад) – резкое нарушение уже сложившегося экономического равновесия [5]. Понятие может проявляться как на отдельных рынках, так и в экономике в целом. Протекание обычно связывается с изменениями на товарном рынке, корректировкой спроса и предложения, что приводит к перепроизводству, снижению цен на конечную продукцию. Это становится основой появления безработицы и банкротства финансового сектора. На рис. 2 представлены фазы экономического цикла [5].

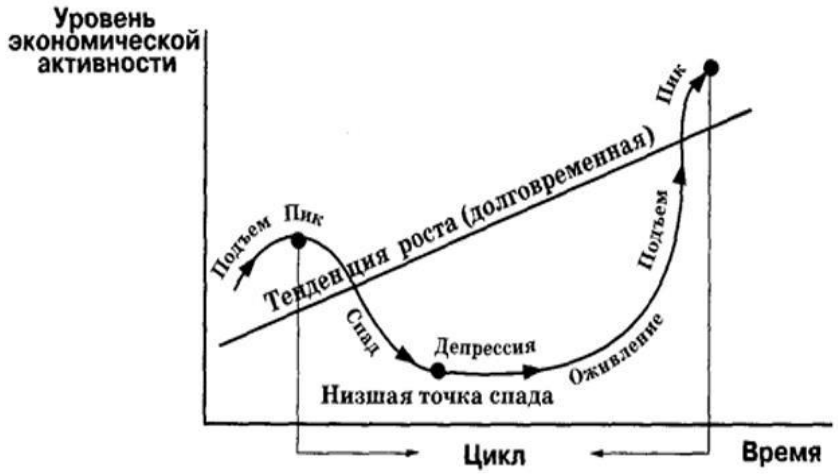

Рисунок 2

Наиболее разрушительной и опасной фазой цикла считается именно кризис. Это связывается с неожиданностью и неопределенностью события как для потребителей, так и для производства. К этой фазе невозможно подготовиться, все случается мгновенно. Именно поэтому на графике его отображают в виде провала. До наступления кризиса экономика процветает и в целом находится в точке равновесия, люди располагают высокими доходами, компании получают хорошую прибыль. После наступает кризис, который разрушает сложившиеся устои.

В момент экономического спада сокращается спрос на товарном и других рынках, тогда как предложение остается на все том же высоком уровне. Фирмы и компании продолжают выпускать собственные товары в огромных количествах, что никак не соотносится со сложившейся обстановкой. Со временем рынок перенасыщается, тогда как спрос еще больше падает. На следующем этапе происходит падение цен, так как предприятиям нужен сбыт и оборачиваемость средств. Отсутствие наличности и проблемы со сбытовой деятельностью приводят к свертыванию воспроизводства. Это становится причиной существенного прироста безработицы и еще большего снижения покупательной способности. Большинство компаний закрывается, как и финансовые институты из-за невыплаты кредитных средств [5].

В состоянии кризиса резко увеличивается предложение на рынке труда, безработица достигает критической отметки. Вложение капитала останавливается, а фирмы остаются неспособными закрывать текущие издержки, оплачивать долги. Здесь наблюдается резкий рост процентной ставки по кредитам. Целый ряд негативных событий, таких как крах фондовой биржи, банкротство предприятий и банков предопределяют конец кризиса, начало депрессии.

Стадия стагнации отличается высокой длительностью и обеспечением равновесия в низшей точке. Депрессия предопределяет новые горизонты развития,

вырабатывает нормы для дальнейшего экономического роста. Наблюдается стабилизация основных показателей макроэкономики, в том числе цен, зарплат на постоянном уровне [5].

При достижении новой равновесной точки рынки восстанавливаются не сразу, так как действия предпринимателей ограничены. Производители боятся потерять собственный капитал из-за очередных колебаний или из-за недостаточности спроса. Со временем позиции в отношении развития бизнеса укрепляются, предприниматели с опаской начинают вкладывать дополнительные средства в развитие производства, торговли и других сфер.

Фаза растягивается в течение длительного периода, являясь самой длительной. Застой зачастую протекает в течение нескольких лет. Чтобы оценить стабилизацию рынка, достаточно наблюдать за ставкой ссудного процента, который постепенно снижается до минимальных значений. Что касается возможностей, то у предпринимателей появляется возможность обеспечить низкие издержки из-за замерших зарплат и стоимости сопутствующих услуг.

Рост производства сопровождается повышением спроса на товары, что также влияет на спрос на других рынках. Следует отметить, что ранее применяемые технологии оказываются недостаточными для нового витка развития, что требует особого внимания к их усовершенствованию, переходу к обновлению систем и подходов. Если такие вложения оказываются удачными, то происходит оживление экономики.

Следующая фаза также именуется экспансией, когда расширяется производство, которое стремится к новой, более высокой равновесной точке. Особое внимание заслуживают средства труда. Именно сюда направляется основной капитал. Оживление также растянуто во времени и сопровождается медленным ростом в зависимости от темпов вложений в экономике. Это также приводит к увеличению цен, росту зарплат и прибылей фирм. Из-за роста возникает потребность в денежных средствах, что приводит к увеличению процентной ставки банков [6].

В представленной стадии нельзя отследить четкие границы, так как различные отрасли экономики могут иметь самый разнообразный тренд, расти через различные отрезки времени. При экспансии все большее количество предпринимателей понимают, что риск полностью соответствует получаемой прибыли. Это приводит к еще большим вложениям, которые косвенно увеличивают благосостояние населения.

В один определенный момент экономические показатели улучшаются, преодолевая производство и доходы предкризисного периода. Эта фаза именуется подъемом, новая точка равновесия – пик. Так как растут цены, осуществляется прирост заработной платы. Вместе с этим начинают применяться другие механизмы, к примеру, контроль темпов роста зарплат к производительности труда. Рынок труда остается основным лимитирующим фактором для последующего роста экономики [5].

Волновое изменение часто соотносится с новшествами на товарном производстве, в средствах труда, при появлении новых предложений на рынке капитала и так далее. В пиковой точке достигается равновесие, которое является наивысшим уровнем возможностей на текущем этапе развития экономики государства. Следует отметить, что на этой стадии также появляется большое количество открытий, но они сопровождаются существенными тратами. Это вновь приводит к перенасыщению рынков и к очередному падению вследствие кризисных явлений. Все это создает парадокс преодоления отдельного кризиса с целью появления нового.

Причины цикличности экономического развития

Развитие теорий цикличности позволило выделить три основных подхода к определению первопричин этого процесса. Первой причиной считается наличие внешних факторов, которые влияют непосредственно на развитие экономики. Экономическая среда является сложной и не замкнутой изнутри, поэтому войны, политические события, разрушительные природные явления и другие активности могут стать причиной вхождения в кризис. Что касается подъемов, то здесь также выделяются внешние факторы, включая технологические прорывы, нахождение новых месторождений ресурсов [7].

Второй первопричиной считаются внутренние факторы, которые протекают в экономическом пространстве. Представленные факторы также могут вызывать рост и падение в зависимости от их особенностей. Ярким примером считается цикличность обновления капитала: оборудование устаревает, и тогда возрастает спрос на новую технику, что повторяется через некоторое время, когда основной капитал вновь изнашивается.

Существуют и другие внутренние факторы, предопределяющие спад или рост экономики: потребительская активность, темпы роста производства, появления новых запасов сырья, работа с инвестициями и поддержкой государства, влияние спроса и потребления благ [7].

Третьей первопричиной появления циклов является совмещение двух вышеописанных. То есть, взаимодействие внешних и внутренних факторов. Согласно этой точке зрения рост на мировом рынке влияет на улучшение состояния на региональном рынке. Миграция повышает возможности для рынка труда, расширяет лимиты воспроизводства для отдельного национального рынка и так далее.

На основании вышесказанного можно сделать вывод, что под экономическим циклом понимается отрезок времени, по прошествии которого происходят падения и подъемы экономической активности, а также связанных макроэкономических характеристик. Ключевая причина их появления связывается с невозможностью поддержания длительного равновесия между совокупным спросом и предложением, расходами и объемами производства.

Цикличность развития экономики можно объяснить только постоянным движением этих величин (рост расходов приводит к подъему, а сокращение становится причиной рецессии). Это касается и изменений предложения при определенном спросе (сокращение приводит к спаду, тогда как прирост к подъему).

Проблема цикличности в российской экономике

Говоря о проблеме цикличности, можно рассмотреть проблему кризисов, а именно причины их возникновения: вызваны ли они естественным ходом экономического развития или же спровоцированы внешними факторами.

С одной стороны, периодический спад деловой активности – это нормальное явление для экономик рыночного типа. Экономическое развитие стран с такой экономикой, в числе которых Россия, сопровождается колебаниями уровня деловой активности, причем эти колебания имеют циклический характер. Несмотря на сложившееся у многих мнение о том, что кризис – это плохо, он в некотором роде оказывает санирующее воздействие на экономику [8].

С другой стороны, затяжные и резко ощутимые спады, происходящие в результате влияние извне, уже являются проблемой для экономики, решение которой во многом зависит от действий государства.

Чтобы оценить цикличность в Российской экономике, нужно проанализировать показатели, определяющие экономический рост страны.

Экономическая цикличность чаще всего рассматривается через анализ динамики реального валового внутреннего продукта (ВВП), который выступает одним из основных агрегированных показателей, характеризующих экономическое развитие. На рис. 3 представлены индексы реального объема ВВП (в процентах к предыдущему году).

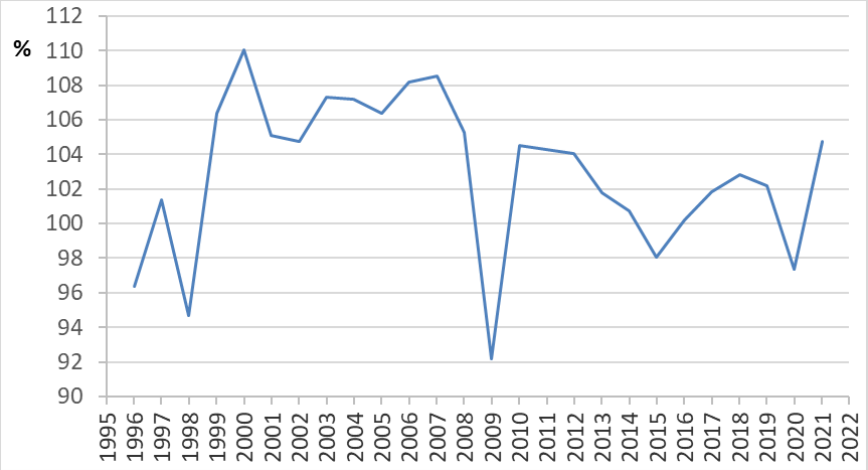

Рисунок 3

На графике изображен темп роста реального ВВП России, по которому можно отследить, в какие годы в стране были спады экономической активности (темпы роста опускались ниже 100 %).

Первоначальный этап рыночных преобразований – «трансформационный спад», через который проходит большинство стран с переходными экономиками.

1998 г. – финансовый и экономический кризис, мнения по поводу причин возникновения неоднородны: от воздействия внешних факторов в виде азиатских кризисов, до серьезных просчетов в денежно-кредитной, налогово-бюджетной и государственной долговой политике России.

Одновременно обрушились котировки на газ и углеводороды. Курсы валют на отечественном рынке отличались высоким ростом. Появилась гиперинфляция, а сбережения населения стремительно обесценились. Предприятия промышленности разорились, возросла безработица.

Итогом этого стала невозможность обслуживания собственных обязательств, что привело к объявлению технического дефолта. Это повлияло на другие макроэкономические сдвиги, приведшие к росту экономики. Страна стала достаточно привлекательной для инвесторов и открытия новых производственных мощностей.

2008-2009 гг. – мировой финансовый кризис, падение цен на нефть. Из-за ипотечного кризиса в США произошло серьезное влияние на все мировое сообщество в виде финансовой и банковской нестабильности. Производство у европейских и американских компаний значительно сократилось. Это также стало причиной снижения цен на углеводороды и другое сырье, что обеспечило минусовой прирост ВВП. Для отечественного рынка произошла девальвация национальной валюты [9].

2014-2016 гг. сопровождается очередным падением цен на нефть, а также введением санкций в отношении Российской Федерации (РФ). Представленная проблема возникла из-за падения спроса на нефтепродукты, а также из-за увеличения добычи последней. Что касается санкций, то они возникли из-за

геополитической ситуации. Рубль упал по отношению к корзине иностранных валют.

Отдельные экономисты указывают, что экономика не смогла в полной мере преодолеть эту кризисную ситуацию. Санкции продолжают наносить непоправимый вред, а курсы остаются на предельно высоком уровне. Что касается роста ВВП, то он прослеживался в перспективе, но с более низкими темпами. 2020 г. отличился пандемией коронавируса, которая стала причиной закрытия границ и свободной торговли. Изоляция населения привела к рецессии, производственный цикл сократился. В это же время наблюдается резкое сокращение спроса на рынках нефтепродуктов. Также имелись негативные факторы, которые связаны с выходом РФ из соглашения Организации стран – экспортеров нефти (ОПЕК). Это стало основой повышения курсов иностранных валют к отечественной.

Проанализировав кризисы 2008-2009, 2014-2016 и 2020 гг. можно сделать вывод, что одной из причин снижения темпов роста ВВП является падение цен на нефть в эти годы [9]. На рис. 4 представлены цены на нефть *Brent* (в долларах США за баррель).

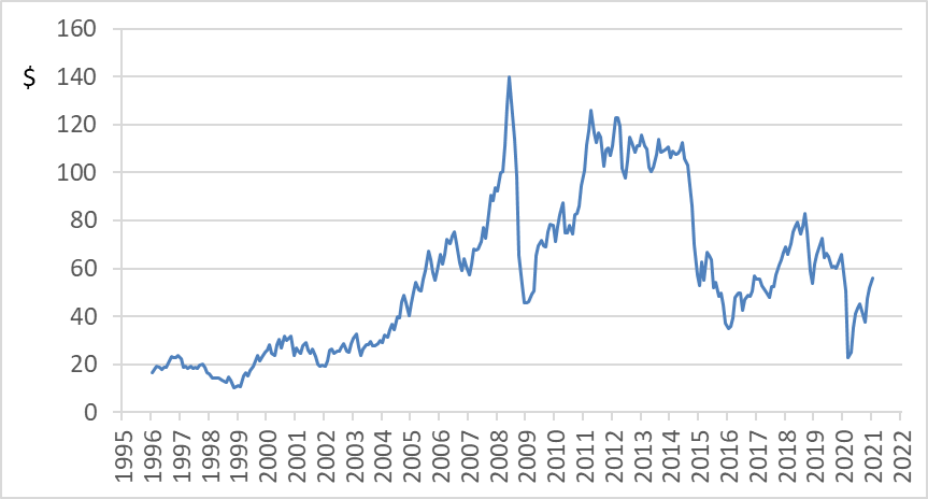

Рисунок 4

Еще одна причина – политические события, которые послужили основным фактором нынешнего кризиса. В феврале-марте 2022 г. произошло резкое ослабление рубля по отношению к иностранным валютам, стоимость доллара Соединенных Штатов Америки (США) выросла до 138 руб. (7 марта 2022 г.).

Стремительно выросли цены на многие группы товаров. 9 марта 2022 г. недельная инфляция в РФ увеличилась до 2,22 %. Столь существенный недельный рост цен стал самым высоким с 1998 г. Большое количество зарубежных компаний ушло с российского рынка: ограничение импорта, остановка заводов, торговых центров, ресторанов, простой и увольнение работников [10].

На основании сказанного выше можно сделать вывод, что основными причинами цикличности в экономики России являются экзогенные факторы. При этом наибольшее влияние оказывают политические и внешнеторговые факторы.

Внешнеторговый фактор основан на торговых колебаниях на мировых рынках, а также на зависимости структуры предлагаемых товаров. Так как основную долю формирования товарооборота составляют энергетические ресурсы (нефть, газ), то любое изменение спроса на них приводит к резкому негативному или позитивному отклику.

Что касается текущего момента, то наибольшее влияние оказывают политические шаги. Они становятся причиной разногласий и невзвешенных

решений, которые приводят к негативным последствиям в экономике. Многие отрасли уже ощутили груз санкций, которые были введены на фоне сложившейся геополитической ситуации.

Вместе с этим, существует и позитивная тенденция, которая предполагает переход на новый уровень через импортозамещение. Тем не менее оценить это с экономической точки зрения весьма проблематично из-за сложности протекающих процессов.

Что касается мировых кризисов, то издержки несет каждая страна. Но в нашем государстве проблема цикличности более выраженная. Последнее проявляется в курсе рубля по отношению к иностранным валютам, формировании бюджета через продажу сырья и так далее.

Причины кризиса 2022 г.

Основной причиной кризиса 2022 г. является сложившаяся геополитическая ситуация, в результате чего странами запада вводятся новые экономические санкции, нацеленные на российский банковский сектор, Центральный банк Российской Федерации (ЦБ РФ), отдельные сектора российской экономики [11].

Для финансовой системы России экономические санкции возымели немедленный эффект. 24 февраля Российский фондовый рынок рухнул на 39 % по индексу РТС. Торги на Московской и Санкт-Петербургской фондовых биржах были приостановлены [11].

26-28 февраля в рамках нового пакета санкций от *SWIFT* было отключено несколько российских банков и около половины золотовалютных резервов Центробанка оказалось заморожено. Начиная с 28 февраля ЦБ РФ прекратил валютные интервенции, мотивировав это санкционной блокировкой своих долларовых и евровых корсчетов.

Платежные системы *Visa* и *MasterCard* приостановили работу в России. Транзакции по картам этих платежных систем недоступны за пределами РФ, а карты, выпущенные за рубежом, не работают в России. Внутри России карты продолжают работать.

Два года пандемии также не прошли даром и оставили массу неблагоприятных последствий в экономике РФ.

Новый этап экономического кризиса в России начался с резкого ослабления российского рубля по отношению к иностранным валютам, что произошло в результате случившихся политических событий и последовавших за этим экономических санкций, нацеленных на российский банковский сектор, Центральный банк РФ, отдельные сектора российской экономики и ряд компаний, а также на высшее руководство России и ряд крупнейших предпринимателей [11].

Особенности цикла на современном этапе экономического развития

На современном этапе становления экономики, природа экономических циклов в значительной степени преобразилась. Характеристика последних выражается следующими основными чертами [12]:

- Каждый последующий кризис преодолевается в более сжатые сроки, однако кризисы стали происходить чаще.
- Цикличность в мировом обществе осуществляется равномерно, что приводит к нахождению отдельных национальных экономик на аналогичных фазах экономического цикла.
- Государственное вмешательство в работу экономики является наиболее важным фактором появления спадов и подъемов (регулирование

государственными инструментами помогает преодолеть спад или продлить стадию роста).

- Между этапами оживления и подъема не существует границы, зачастую они являются одной огромной фазой (в некоторых источниках все это именуется расширенной фазой производства).

Рассмотренные выше особенности зачастую связываются с тремя временными лагами [12]:

- Цикл Китчина (предполагает возникновение разрыва между выделением инвестиций и использованием новых средств труда).
- Цикл Жюгляра (в этом случае колебания основаны на вводе и выбытии активной части основных производственных фондов).
- Циклы Кузнеца и Кондратьева (колебания происходят из-за обновления пассивной части основных производственных фондов).

Основная зависимость базируется на инвестициях. Процесс воспроизводства и реновация инвестиционных товаров лежат в основе циклов. Поэтому высокая скорость технологического развития и износ основных средств предопределяют современные экономические циклы.

Заключение

Исследование цикличности экономического развития позволяет сделать несколько важных выводов. Во-первых, экономические циклы являются неотъемлемой частью рыночной экономики, обусловленной множеством внутренних и внешних факторов, включая технологические инновации, государственное регулирование, внешнеторговую деятельность и политические события. Во-вторых, несмотря на значительное количество исследований, до сих пор не существует единой теории, которая бы объясняла все аспекты и механизмы экономических циклов, что указывает на необходимость дальнейших исследований в данной области.

Особое внимание в работе было уделено анализу цикличности в российской экономике, где кризисные явления часто обусловлены как внутренними, так и внешними факторами, среди которых значительное место занимают колебания мировых цен на энергоресурсы и геополитическая обстановка. Кризис 2022 г., вызванный рядом внешних санкций и политических событий, стал ярким примером влияния экзогенных факторов на экономику страны.

В заключение можно сказать, что понимание механизмов и причин экономических циклов имеет критическое значение для разработки эффективных государственных политик, направленных на смягчение негативных последствий экономических спадов и стимулирование устойчивого развития. Это предполагает не только анализ исторического опыта и существующих теоретических подходов, но и постоянный поиск новых методов управления экономической активностью на макро- и микроуровнях. Важным аспектом является также учет специфики национальной экономики и международного контекста, в котором она функционирует.

Литература

1. Глазьев С.Ю. О новой парадигме экономической науки // Экономическая наука современной России. Ч. 2, 2016. – № 4. – С. 10-21.
2. Днепров М.Ю. Экономическая теория: учебник для вузов. – М.: Издательство Юрайт, 2020. – 216 с.

3. Полякова Е.М. Экономическая теория: Учебное пособие для обучающихся всех форм обучения, всех направлений подготовки ПГСХА. – 2-е изд., перераб. и доп. – Уссурийск: ФГБОУ ВО ПГСХА, 2019. – 310 с.
4. Коннина Е.С. Циклическое развитие экономики – объективное явление // Материалы IX Международной студенческой научной конференции «Студенческий научный форум», 2020. – 20 с.
5. Башкирова В.Е. Развитие экономики РФ в условиях современного кризиса. Экономические циклы. Экономический рост [Электронный ресурс] // Современные научные исследования и инновации, 2016. – № 2. – Режим доступа: https://web.snauka.ru/issues/2016/02/64775, свободный.
6. Аришкина О.Д. Кризисы мировой экономики. – М.: Экономикс, 2017. – 189 с.
7. Старидце И.И. Мировая экономика: кризисы и пути их преодоления. – М.: Экономикс, 2017. – 234 с.
8. Морозова С.А. Мировые экономические кризисы: анализ особенностей, причин, последствий и мер преодоления // Вопросы устойчивого развития общества, 2020. – № 9. – С. 86-90.
9. Дмитриев Н.И. Мировая экономика: причины кризисных явлений. – СПб.: Питер, 2017. – 306 с.
10. Фадеева И.С. Развитие мировой экономики: динамика, прогнозы, риски и пути их преодоления // Социально-экономический и гуманитарный журнал Красноярского ГАУ, 2019. – № 2 (12). – С. 3-13.
11. Официальный сайт Центрального Банка Российской Федерации [Электронный ресурс]. – Режим доступа: https://cbr.ru, свободный.
12. Устинова Д.А. Особенности циклического развития экономики // Молодой ученый, 2016. – № 19 (123). – С. 530-533.

ЦИКЛИЧНОСТЬ ЭКОНОМИЧЕСКОГО РАЗВИТИЯ И АНТИКРИСИЗНАЯ ПОЛИТИКА В РОССИЙСКОЙ ФЕДЕРАЦИИ

В.Д. Зюзин, *Нижегородский государственный университет им. Лобачевского, v.d.zyuzin@gmail.com;*
Н.А. Башмуров, *Нижегородский государственный университет им. Лобачевского, bashmurov.nikolai@yandex.ru;*
М.Д. Зюзина, *Вознесенская СОШ, mariazyu@mail.ru.*

УДК 338.2:336.1

Аннотация. В данной статье рассматривается актуальная проблема цикличности экономического развития, которая играет ключевую роль в динамике мировой экономики. Целью исследования является анализ основных аспектов циклических колебаний в экономике, характеристик экономических циклов на современном этапе развития, а также изучение антикризисной политики РФ и разработка предложений по выходу из кризисной ситуации. Работа основывается на теоретическом анализе экономической литературы и практическом изучении антикризисных мер, применяемых в РФ. В ходе исследования были проанализированы различные подходы к пониманию экономических циклов, а также проведен анализ эффективности антикризисных мер, принятых российским правительством и Центральным банком РФ. В результате работы предложены конкретные шаги для структурной трансформации экономики России,

направленные на минимизацию негативных последствий кризисных явлений и на поиск новых путей для стабильного экономического развития. Исследование показывает, что успешный выход из кризиса требует комплексного подхода, включающего изменение производственных и логистических цепочек, применение передовых технологий и активизацию предпринимательской деятельности при поддержке государства.

Ключевые слова: экономические циклы; антикризисная политика; структурная трансформация; Российская Федерация; цикличность экономического развития; кризис и восстановление; макроэкономическое регулирование; инвестиционные стратегии; технологическое развитие; импортозамещение.

ECONOMIC DEVELOPMENT CYCLICITY AND ANTI-CRISIS POLICY IN THE RUSSIAN FEDERATION

Vladislav Zyuzin, *Nizhny Novgorod State University Lobachevsky;*
Nikolay Bashmurov, *Nizhny Novgorod State University named after N.Y. Lobachevsky;*
Mariya Zyuzina, *Voznesenskaya Secondary School.*

Annotation. This research paper addresses the critical issue of economic development cyclicity, which plays a vital role in the dynamics of the global economy. The study aims to analyze the main aspects of economic fluctuations, characteristics of economic cycles at the current stage of development, and examine the anti-crisis policy of the Russian Federation, proposing solutions for crisis situations. The work is based on theoretical analysis of economic literature and practical study of anti-crisis measures implemented in Russia. Various approaches to understanding economic cycles were analyzed, as well as the effectiveness of anti-crisis measures adopted by the Russian government and the Central Bank of the Russian Federation. The research proposes specific steps for the structural transformation of Russia's economy, aimed at minimizing the negative effects of crisis phenomena and seeking new ways for stable economic development. The study shows that successful crisis recovery requires a comprehensive approach, including changes in production and logistics chains, application of advanced technologies, and activation of entrepreneurial activity with state support.

Keywords: economic cycles; anti-crisis policy; structural transformation; Russian Federation; economic cycle cyclicity; crisis and recovery; macroeconomic regulation; investment strategies; technological development; import substitution.

Введение

Человечество неустанно стремится к улучшению своего благополучия и качества жизни, что напрямую связано с экономическим прогрессом. Однако экономический рост не может быть бесконечным; периоды спада и нестабильности неизбежны. Изучая экономическую историю последних нескольких столетий, можно увидеть множество примеров нестабильности рыночной экономики. После этапов роста и развития, когда достигается экономический успех, следуют периоды спада и рецессии, характеризующиеся сокращением производства и увеличением безработицы. Экономика развивается циклично, при этом каждый новый этап стимулируется научно-техническими инновациями.

Эта тема является одной из наиболее сложных в макроэкономике из-за отсутствия единой теоретической базы и наличия множества подходов и методов, в том числе математических. Первые попытки теоретического анализа экономического роста были предприняты в начале *XIX* века, когда экономисты начали замечать цикличность с ее спадами и подъемами. Проблема циклического

развития экономики привлекла внимание многих ученых, включая Туган-Барановского, К. Маркса, Кейнса, Кондратьева.

Большинство теорий содержит элементы неопределенности, часто используя формулировки типа «вероятно» или «возможно». В работе «Макроэкономика. Глобальный подход» отмечается, что на данный момент не существует универсальной экономической теории, признанной всеми специалистами, что представляет собой значительную проблему для современных исследований.

Целью данной научной работы является анализ ключевых аспектов цикличности экономического развития. Для достижения этой цели предстоит выполнить следующие задачи:

- исследовать антикризисную политику Российской Федерации;
- разработать рекомендации по преодолению кризиса.

Проблемы и перспективы экономического развития

Антикризисная политика РФ

Антикризисная политика – это комплекс мер, направленный на снижение негативного эффекта распространения кризисных явлений, уменьшение их продолжительности и глубины. Для этого существует огромное количество инструментов, а основным регулятором осуществления антикризисной политики считаются Центральный банк Российской Федерации (ЦБ РФ) [2] и Правительство РФ. Именно эти органы власти определяют необходимые антикризисные меры как на финансовом рынке, так и на потребительском. Определение рычагов воздействия зависит от особенностей протекания кризиса, его глубины.

На текущий момент Российская Федерация находится в экстремальных условиях, вызванных санкциями со стороны других государств. Для обеспечения защиты использовались самые разнообразные антикризисные меры, которые раскрыты далее.

С 1 мая 2022 г. все семьи со среднедушевым доходом ниже прожиточного минимума, воспитывавшие детей от 8 до 16 лет (включительно), могли подать заявление на получение нового пособия. И хотя заявление подавалось не раньше мая, выплату назначили с апреля. Ее сумма составила 50, 75 или 100 % регионального прожиточного минимума на ребенка, в зависимости от среднедушевого дохода семьи.

Для получения пособия взрослые члены семьи должны были работать официально, или у них должна была быть уважительная причина отсутствия работы. Также учитывалось имущество членов семьи, в том числе наличие машины, гаража, земельного участка и вклада в банке.

В конце марта 2022 г. президент РФ подписал закон, который отменил налог на доходы физических лиц (НДФЛ) с процентов по банковским вкладам и счетам, полученных в 2021-2022 гг. Налог с купонов облигаций пришлось платить [3].

Водители, у которых срок удостоверения истекал в 2022-2023 гг., могли не беспокоиться о продлении документа. Все российские водительские удостоверения были продлены на три года автоматически.

Был отменен повышенный транспортный налог на машины, считавшиеся роскошными, для автовладельцев, чье авто не дороже 10 млн руб. Для них транспортный налог, исчисляемый за 2022 г., был рассчитан без повышающих коэффициентов [3].

С марта 2022 г. банки могли продавать физлицам драгметаллы в слитках без НДС по ставке 20 %. Драгметаллы стали хорошей инвестиционной заменой валюте.

Было приостановлено выселение должников. Центробанк рекомендовал банкам, микрофинансовым организациям, кредитным потребительским кооперативам, сельскохозяйственным кооперативам и жилищным накопительным кооперативам не выселять до конца 2022 г. людей, на жилье которых было обращено взыскание.

Был увеличен порог беспошлинной покупки в зарубежных интернет-магазинах. С прежних 200 евро беспошлинный порог увеличили до 1000 евро. Требования к весу остались прежними – до 31 кг. Лимит беспошлинного ввоза был увеличен лишь до 1 октября 2022 г.

Заемщики-физлица, заключившие договора кредита и займа до 1 марта 2022 г., могли обратиться к кредитору за полугодовой отсрочкой платежей. Заемщик должен был подтвердить снижение своего дохода более чем на 30 % по сравнению с аналогичным периодом прошлого года.

Сумма кредита (займа) не должна была превышать максимальную сумму, установленную правительством РФ. Это было 300 тыс. руб. по потребительским кредитам и от 3 до 6 млн руб. по ипотеке, в зависимости от региона.

Был введен мораторий на банкротство, действовавший для граждан, юридических лиц и предпринимателей с 1 апреля по 1 октября 2022 г. Исключение составили застройщики многоквартирных домов, входящие в реестр проблемных объектов.

В течение срока действия моратория кредиторы не могли подавать заявления на банкротство должников. Но у самих должников право на подачу такого заявления оставалось.

Был упрощен порядок признания дипломов для граждан, обучавшихся в вузах на территории недружественных стран. Если в России уже когда-то признавался такой же диплом, полученный в определенной стране, то и в данном конкретном случае его признают.

Студенты, которым пришлось прервать обучение за границей, могли приехать в Россию и продолжить обучение в ведущих университетах РФ бесплатно. Студентов принимали как на бюджет, так и на платные места, при этом вуз получал компенсацию. Курс, на который зачисляли студента, зависел от его достижений в иностранном вузе.

На три года ИТ-компании, аккредитованные Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры РФ) [4], были освобождены от налоговых проверок и других видов муниципального контроля. До конца 2024 г. ставка по налогу на прибыль для них составила 0 процентов.

Для реализации новых проектов и обеспечения текущих ИТ-компании могли брать кредиты под 3 % годовых.

Специалисты, задействованные в ИТ-индустрии, получили право на отсрочку от службы в армии до 27 лет, но только на период работы в аккредитованной ИТ-компании. Также они получили возможность взять ипотеку на льготных условиях. Аккредитованные ИТ-компании получили средства, которые пошли на улучшение жилищных условий отдельных сотрудников и повышение их зарплаты.

Предприниматели, входящие в единый реестр субъектов малого и среднего предпринимательства, были избавлены от плановых налоговых проверок до начала 2023 г. [3].

Субъектам малого и среднего бизнеса возместили расходы за использование системы быстрых платежей (СБП) в период с 1 января до 1 июля 2022 г.

Был легализован параллельный импорт товаров. Список таких товаров был сформирован Минпромторгом.

До начала лета 2022 г. счета за долги не блокировались. До 1 июня инспекторы Федеральной налоговой службы (ФНС) [3] не выносили решения о блокировке счетов при взыскании долгов.

Был сокращен срок регистрации общества с ограниченной ответственностью (ООО) и индивидуального предпринимательства (ИП). Через сервис «Государственная онлайн-регистрация бизнеса» можно было зарегистрировать ИП или ООО всего за день. Документы должны были быть заверены квалифицированной электронной подписью, которую можно было получить в любом удостоверяющем центре – их перечень есть на сайте Минцифры РФ [4].

Работодатель, трудоустроивший соискателя моложе 30 лет, предложенного Центром занятости, получал 54 000 руб. Подать заявку на получение субсидии можно было в Фонд социального страхования Российской Федерации (ФСС РФ) до 15 декабря 2022 г., но не ранее чем через месяц с того момента, как работник приступил к своим обязанностям.

НДС можно было вернуть из бюджета еще до окончания камеральной проверки – «авансом», в течение 11 рабочих дней после подачи заявления в ФНС [3].

Штрафа за отсутствие бумажного чека не было. Из-за нарушения логистических цепочек у российских компаний возникли проблемы с приобретением бумажной чековой ленты. Поэтому за ее отсутствие штрафовать не стали. ФНС советовала продавцам направлять покупателям электронные чеки на электронную почту или по номеру телефона.

Был утвержден перечень пострадавших отраслей экономики РФ. Правительство составило экономический перечень, в который входили более 70 кодов общероссийского классификатора видов экономической деятельности (ОКВЭД). Участники этих отраслей смогли воспользоваться кредитными каникулами на полгода – взять отсрочку по возврату кредита или уменьшить размер платежей.

Владельцы малого бизнеса могли взять кредит (или рефинансировать текущий) на срок до 1 года и без ограничений по цели кредитования. Сумма – до 300 млн руб., и ставка не выше 15 % годовых. Для представителей среднего бизнеса сумма повысилась до 1 млрд руб. и со ставкой до 13,5 % годовых.

В программе участвовали банки: ПАО Сбербанк, Банк ВТБ (ПАО), АО «АЛЬФА-БАНК», АО «Россельхозбанк», ПАО Банк «ФК Открытие», ПАО «АК БАРС» БАНК, ПАО «Промсвязьбанк», ПАО «Совкомбанк», АО «БКС Банк», АО «ВЛАДБИЗНЕСБАНК», АКБ «Держава» ПАО, АО «Кредит Европа Банк (Россия)», Банк «Левобережный» (ПАО), ПАО АКБ «Металлинвестбанк», АО АКБ «МЕЖДУНАРОДНЫЙ ФИНАНСОВЫЙ КЛУБ», АО Банк «Национальный стандарт», ПАО «НБД-Банк», АО Банк «Объединенный капитал», АО «Ури Банк», АО КБ «Хлынов», АО АКБ «ЦентроКредит».

Таким образом, мы видим, что ведется активная антикризисная политика, направленная на поддержку практически всех сфер жизни общества и касающаяся как физических, так и юридических лиц.

Пути выхода из кризиса

Кризисная ситуация в экономике страны будет ухудшаться вне зависимости от принятых мер, любой сценарий будет отличаться масштабными потерями в сравнении с кризисом при коронавирусе. Стоит отметить, что серьезный удар по

экономике больше связывается с уходами брендов и со сворачиванием производства, чем от прямых санкций в действии [5].

В марте 2022 г. отечественная экономика попала в фазу спада, что связывается с серьезным санкционным давлением и сворачиванием деятельности иностранных компаний. Если проводить параллели с проблемой 2020 г., когда началось сворачивание деловой активности из распространения коронавируса, то здесь нужно указать на более обширные последствия вне зависимости от выбранного сценария и реализуемых мероприятий.

Сокращение связей с иностранным производством и инвесторами зачастую соотносится с имиджевыми потерями. Такое явление нанесло удар по логистическим цепочкам, что повлияло как на поставку товаров конечного потребления, так и на производственные узлы или комплектующие. Из-за сложности этих цепочек, большого участия поставщиков, проблемы могут возникать сразу в нескольких точках. В результате этого российская экономика не может работать в новых условиях, испытывая шок и проваливаясь в кризис. Это показывает, что не только санкции наносят вред, но и прямой уход международных корпораций.

В настоящее время о спаде экономической активности говорят только опросы предприятий, а оперативные экономические индикаторы его не показывают. Во многом это объясняется наличием запасов сырья и материалов у части производителей. В розничной торговле в марте-апреле 2022 г. и вовсе наблюдался рост оборота на фоне временного всплеска потребления.

Однако статистика внешнеторговых потоков указывает на ухудшение [5]: стоимостные объемы импорта и объемы входящих рублевых платежей в отрасли-экспортеры заметно снижаются. Также снижаются объемы железнодорожных грузоперевозок. Опросы предприятий начинают фиксировать нарастание негативных явлений в экономике, которые будут распространяться через производственные цепочки и снижение спроса.

Таким образом, для выхода из кризиса российской экономике необходима «структурная трансформация». Несмотря на то, что трансформация в условиях продолжительного действия внешних ограничений будет сопровождаться технологическим регрессом в ряде отраслей при одновременном росте производства инвестиционных товаров и технологий, ее эффект со временем, станет ощутим для экономики РФ.

«Структурную трансформацию» российской экономики авторы считают необходимым осуществить в четыре этапа. Рассмотрим подробнее каждый этап:

1. Изменение логистических и производственных цепочек. Для этого необходим поиск поставщиков, способных обеспечить схожие по характеристикам и функциональному назначению товары, а также формирование собственных возможностей для замены отдельных узлов и агрегатов. По возможности обеспечить эффективное использование имеющихся запасов. На этом этапе возникает потребность в выстраивании новых маршрутов.

Основной задачей для управленческого аппарата властных структур является минимизация масштаба спада, который возникает из-за перестройки цепочек, прокладывания новых маршрутов. В этом направлении государство обязано взять часть рисков финансового рынка на себя.

2. Перестройка компаний и организаций к работе в новых условиях формирования производственных и распределительных цепочек. Как только запасы будут исчерпаны, а большинство производственных цепочек перестанут работать, нужно определить новые физические возможности для восстановления последних. Здесь уже требуется полная переориентация на новых поставщиков и

рынки для удовлетворения функций производства. Этот этап также связывается с рядом негативных эффектов, которые выражаются через повышение безработицы и снижение доходов.

В числе прочего на этом этапе «возрастет роль небольших посреднических внешнеторговых компаний и «челночного» малого бизнеса (особенно в потребительском сегменте). Однако малые объемы закупок и усложнение логистики приведут к удорожанию такого импорта и невозможности в полном объеме заменить традиционных поставщиков.

Спад объемов производства и валовой добавленной стоимости произойдет в основном на первом и втором этапах.

3. Третий этап является наиболее сложным и важным. Предполагает проведение индустриализации производства и рынка через применение передовых технологий. Представленный этап может занимать существенное время, так как требует реализации определенных инвестиционных проектов. Здесь также важно понятие импортозамещения, в том числе в сфере техники и технологий. Здесь уже возникает стабильность роста производства, но с изменением технологического уровня.

Кроме того, эффект малого масштаба (невозможность массового производства в условиях ограниченного объема российского рынка) приведет к удорожанию такой техники и технологий относительно более современных, но недоступных технологий.

Таким образом, техническая и экономическая эффективность созданной техники будет уступать нынешним. В частности, это затронет уровень цифровизации техники и бизнес-процессов, где технологический откат окажется наиболее выраженным.

Возврат экономики на траекторию роста на данном этапе будет способствовать снижению общеэкономической неопределенности, восстановлению кредитной активности и закрытию отрицательного разрыва выпуска. Это предполагает временное превышение потенциальных темпов роста. В свою очередь меньшая производительность и эффективность техники и технологий потребует увеличения числа занятых в отраслях, использующих технику и технологии, а также в отраслях, их обслуживающих.

Это снизит общий уровень безработицы, но слабо повлияет на уровень реальных зарплат. Поэтому рост зарплат будет отставать от роста производства, а труд станет дешеветь относительно капитала (основных фондов).

4. Завершающий этап, который обеспечивает завершение процесса перестройки. Именно здесь появляется возможность достигнуть точки равновесия через использование более совершенных технологий. Будут наблюдаться различные технологические прорывы по отраслям экономики.

Потенциальные темпы прироста могут оказаться немного ниже, чем это было ранее, однако они будут положительными. Это указывает на тот факт, что в среднесрочном периоде российская экономика сможет укрепить экономическое положение в сфере производства, бизнес-услуг и так далее, обретут равновесие и цены.

Следует понимать, что успешность прохождения рассматриваемых этапов в полной мере зависит от активности предпринимателей. Поэтому перед властными структурами ставится ключевая задача в обеспечении государственной поддержки предпринимательской деятельности. Это может связываться с либерализацией рынка, снижением уровня контроля, сокращением налоговых ставок.

Заключение

Особое внимание в работе уделено антикризисной политике РФ, включающей широкий спектр мер – от поддержки физических лиц и бизнеса до структурных реформ в экономике. Было выявлено, что, несмотря на значительные усилия государства, необходима дальнейшая адаптация и развитие инструментария антикризисного управления для повышения его эффективности и гибкости в условиях постоянно меняющейся внешней и внутренней среды.

На основании проведенного анализа предложена концепция «структурной трансформации» экономики России, направленной на устойчивое развитие и снижение уязвимости перед кризисными явлениями. Трансформация предполагает переосмысление и оптимизацию производственных и логистических цепочек, активное внедрение инновационных технологий, поддержку предпринимательства и создание благоприятных условий для инвестирования.

Литература

1. Глазьев С.Ю. О новой парадигме экономической науки // Экономическая наука современной России. Ч. 2., 2016. – № 4. – С. 10-21.
2. Официальный сайт Центрального Банка Российской Федерации [Электронный ресурс]. – Режим доступа: https://cbr.ru, свободный.
3. Официальный сайт Федеральной налоговой службы РФ [Электронный ресурс]. – Режим доступа: https://www.nalog.gov.ru/rn77/, свободный.
4. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/, свободный.
5. Тумгоев М.У. Пути выхода из экономического кризиса в современных условиях // Экономика и бизнес: теория и практика, 2020. – № 7. – С. 234-239.
6. Моисеев, В. В. Антикризисная политика России // Вестник БГТУ имени В. Г. Шухова, 2016. – № 7. – С. 181-186.
7. Тумгоев М.У. Кризисные явления в экономики России и пути их предопределения. – М.: Перо, 2018. – 220 с.
8. Тумгоев М.У. Пути выхода из экономического кризиса в современных условиях // Экономика и бизнес: теория и практика, 2020. – № 7. – С. 234-239.
9. Официальный сайт акционерного общества «Инвестиционная компания «ФИНАМ» [Электронный ресурс]. – Режим доступа: https://www.finam.ru, свободный.
10. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/, свободный.
11. Официальный сайт Федеральной налоговой службы РФ [Электронный ресурс]. – Режим доступа: https://www.nalog.gov.ru/rn77/, свободный.
12. Официальный сайт Федеральной службы государственной статистики РФ [Электронный ресурс]. – Режим доступа: https://rosstat.gov.ru, свободный.

СИСТЕМЫ, СЕТИ И УСТРОЙСТВА СВЯЗИ. РАДИОТЕХНИКА. АНТЕННЫ. ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА. ПРИБОРЫ И МЕТОДЫ ИЗМЕРЕНИЯ. МЕТРОЛОГИЯ

ИСПОЛЬЗОВАНИЕ SDR-ТЕХНОЛОГИИ ДЛЯ ЗАДАЧ СЕТЕВОГО ПОЗИЦИОНИРОВАНИЯ: РЕАЛИЗАЦИЯ КАНАЛА ПЕРЕДАЧИ И ПРИЕМА НАВИГАЦИОННЫХ ДАННЫХ

Г.А. Фокин, *д.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича, grihafokin@gmail.com;*
К.Е. Рютин, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича, ryutin.sut@gmail.com.*

УДК 621.396.969

Аннотация. В последние годы проблема развития технологии сетевого позиционирования в условиях отсутствия сигналов глобальной навигационной спутниковой системы стала весьма актуальной. В данной работе формализованы, программно реализованы и экспериментально апробированы процедуры сбора, кодирования, передачи, приема, обработки и визуализации собственных глобальных координат базовых станций.

Ключевые слова: позиционирование; программно-конфигурируемое радио; *LTE*; передача данных; экспериментальная апробация.

SOFTWARE-DEFINED RADIO NETWORK POSITIONING TECHNOLOGY DESIGN: IMPLEMENTATION OF THE NAVIGATION DATA TRANSMISSION AND RECEIVING CHANNEL

Grigoriy Fokin, *Doctor of Technical Sciences, Associate Professor, St. Petersburg State University of Telecommunications named after Prof. Bonch-Bruevich;*
Konstantin Ryutin, *St. Petersburg State University of Telecommunications named after Prof. Bonch-Bruevich.*

Annotation. The problem of developing network positioning technology in Global navigation satellite system denied environment, has become highly relevant in the past years. In the present study, the procedures for base stations own navigation data acquisition, coding, transmission, reception, processing and visualization are formalized, implemented in software and experimentally verified.

Keywords: positioning; software-defined radio; *LTE*; data transmission; experimental validation.

Введение

В последние годы возникновение научно-исследовательских инициатив в области развития технологии сетевого позиционирования с использованием программного-конфигурируемого радио (*SDR – Software-Defined Radio*) объясняется отсутствием полного покрытия сигналами глобальной навигационной спутниковой системы (ГНСС) в условиях плотной городской застройки, где наиболее востребована услуга точного определения местоположения [1-10].

Разработанный лабораторией программно-конфигурируемого радио в Санкт-Петербургском государственном университете телекоммуникаций им. проф.

М.А. Бонч-Бруевича прототип технологии определения местоположения пользовательского устройства (*UE – User Equipment*) в сети стандарта *LTE* (*Long-Term Evolution*) [11-17] использует разностно-дальномерный метод позиционирования *OTDOA* (*Observed Time Difference Of Arrival*) [18-20], специфицированный в стандартах *LTE* [21] и 5*G* [22]. Экспериментальная апробация разработанного прототипа доказала возможность достижения дециметровой точности определения местоположения *UE* с использованием метода *OTDOA* [16]. В отличие о стандартизированного подхода на основе измерений по опорным сигналам позиционирования (*PRS – Positioning Reference Signals*), разработанный и экспериментально апробированный прототип использует только сигналы первичной (*PSS – Primary Synchronization Signal*) и вторичной (*SSS – Secondary Synchronization Signals*) синхронизации, а также опорные сигналы сот (*CRS – Cell-specific Reference Signal*). Таким образом, реализованный подход позволяет решить задачу позиционирования без необходимости для *UE* становиться абонентом какого-либо мобильного оператора.

Для дальнейшей апробации разработанного прототипа технологии сетевого позиционирования в глобальной системе координат (СК) необходимо реализовать приемопередачу собственных глобальных координат *SDR*-макетов базовых станций (*eNB – eNodeB*) вместе с опорными сигналами, по которым *UE* выполняет измерения разностей дистанций. Это позволит *UE* преобразовать результаты оценки координат (ОК) из локальной в глобальную СК.

Решение данной задачи начинается с получения от ГНСС-приемника на стороне макета *eNB* глобальных координат в формате *NMEA* (*National Marine Electronics Association*) [23] и дальнейшего кодирования их в соответствии с универсальным форматом представления навигационной информации в 3*GPP*-сетях (*GAD – Geographical Area Description*) [24]. Затем глобальные координаты в формате *GAD* должны быть переданы *eNB* вместе с опорными сигналами *CRS* и получены на стороне макета *UE*.

Материал данной статьи организован следующим образом: во втором разделе формализованы процедуры получения навигационных данных в формате *NMEA*, кодирования их в формат *GAD* и обработки в транспортном и физическом каналах *LTE*; в третьем разделе формализованы процедуры приема сигнала *LTE* из эфира, обработки его в физическом и транспортном каналах *LTE*, декодирования пакета *GAD* и отображения координат на карте в глобальной СК; в четвертом разделе приводится экспериментальная апробация разработанного приемопередатчика навигационных данных в лабораторных условиях.

Процедуры передачи навигационных данных

Перед кодированием и обработкой навигационных данных в каналах *LTE* они должны быть сначала получены ГНСС-приемником по протоколу *NMEA*, затем разобраны и закодированы в пакет данных, определенный форматом *GAD* [24]. Далее пакет навигационных данных с координатами *eNB* кодируется в транспортном и обрабатывается в физическом каналах *LTE*, модулируется и передается в эфир. Рисунок 1 иллюстрирует обобщенную последовательность процедур передачи навигационных данных. Ниже приводится подробное описание каждого блока процедур.

Рисунок 1

Процедуры приема и разбора данных *NMEA*

Получение глобальных координат *eNB* может быть выполнено с помощью любого ГНСС-приемника, который передает полученные данные через последовательный порт по протоколу *NMEA* [23]. Протокол *NMEA* поддерживает множество форматов представления навигационной информации, однако самым подходящим для решения поставленной задачи является формат *GGA*, который передает информацию о последнем зафиксированном местоположении ГНСС-приемника. В этом формате также присутствует флаг «*GPS Quality Indicator*», который сигнализирует о валидности полученных координат. Таким образом, при запуске программы происходит инициализация ГНСС-приемника через последовательный порт, затем запускается бесконечный цикл, условием окончания которого является получение *NMEA*-пакета в формате *GGA* с установленным флагом «*GPS Quality Indicator*». Далее происходит разбор полей полученного *NMEA*-пакета и преобразование координат в формат десятичных градусов. Полученные значения широты, долготы и высоты передаются в модуль кодирования в пакете *GAD*. Рисунок 2 иллюстрирует обобщенный алгоритм приема и разбора навигационных данных от ГНСС-приемника.

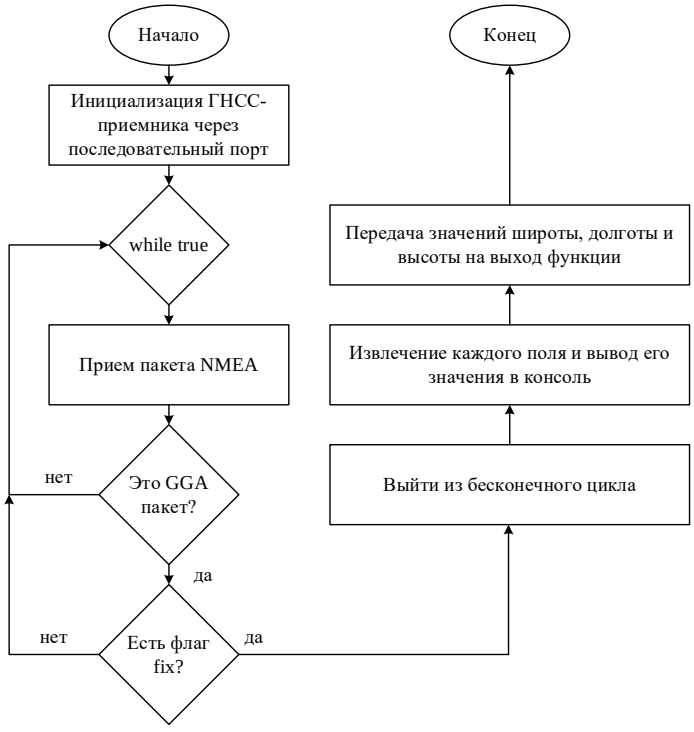

Рисунок 2

Процедуры кодирования навигационных данных в формат *GAD*

Широкий спектр сценариев позиционирования в сетях стандартов *LTE* и 5*G*, а также неоднородность линий положения различных методов ОК, основанных на измерениях дальностей, разностей дальностей и углов прихода сигналов, обуславливают необходимость корректного представления и преобразования форматов ОК. Спецификация 3*GPP TS* 23.032 [24] определяет правила кодирования, представления и преобразования форматов ОК для различных технологий сетевого позиционирования. Для кодирования навигационных данных в пакет *GAD* используется формат точки эллипсоида высокой точности с высотой и эллипсоидом неопределенности (*High Accuracy Ellipsoid point with altitude and uncertainty ellipsoid*). Формирование пакета данных в этом формате описано в [24].

Процедуры кодирования в транспортном канале *LTE*

После формирования пакета навигационных данных его необходимо закодировать и обработать на транспортном (*DL-SCH – DownLink Shared CHannel*) и физическом (*PDSCH – Physical Downlink Shared CHannel*) уровнях *LTE*, соответственно. Физический нисходящий разделяемый канал *PDSCH* используется для передачи нисходящего разделяемого канала *DL-SCH*. В свою очередь, *DL-SCH* – это транспортный канал, используемый для передачи нисходящих данных (транспортных блоков). В формировании пакета данных в транспортном канале *DL-SCH* участвуют следующие процедуры: 1) добавление контрольной суммы к исходному блоку данных; 2) сегментация блока данных, если он превышает максимальный размер, определенный спецификацией; 3) помехоустойчивое канальное турбо-кодирование; 4) согласование скорости; 5) объединение сегментированных блоков данных. Рисунок 3 иллюстрирует диаграмму последовательности процедур кодирования пакета *GAD* в транспортном канале *DL-SCH*.

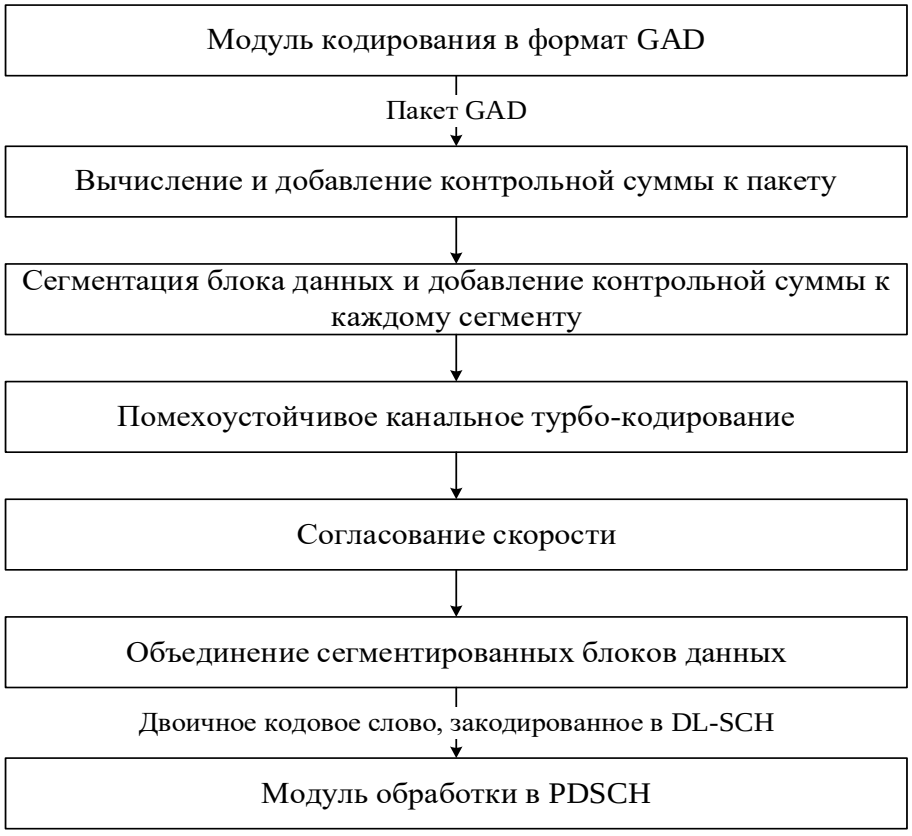

Рисунок 3

Процедуры обработки в физическом канале *LTE*

Обработка транспортного блока данных канала *DL-SCH* в физическом канале *PDSCH* выполняется согласно следующим процедурам: 1) скремблирование; 2) модуляция (формирование комплексных символов); 3) распределение комплексных символов одному уровню или нескольким параллельным уровням; 4) прекодирование (преобразование информации в соответствии с алгоритмами *MIMO*).

Стандарт *LTE* позволяет обрабатывать более одного кодового слова параллельно. Рисунок 4 иллюстрирует диаграмму последовательности процедур обработки блока данных в физическом канале *PDSCH*.

После формирования комплексных модулированных символов их необходимо отобразить на частотно-временной ресурсной сетке *OFDM* (*Orthogonal Frequency Division Multiplexing*) кадра. Во избежание ухудшения результатов работы корреляторов по *CRS*, для размещения на ресурсной сетке были выбраны индексы символов, в которых *CRS* не размещаются вовсе, а также размещение выполнялось в самой маленькой полосе – 1,4 МГц для гарантированного доступа к навигационной информации при работе в любой полосе. После размещения символов на ресурсной сетке формируется *OFDM*-сигнал во временном домене с помощью обратного быстрого преобразования Фурье (*ОБПФ*). Далее происходит инициализация *SDR*-платформы и передача в эфир полученного *OFDM*-сигнала.

Рисунок 5 иллюстрирует диаграмму последовательности процедур формирования ресурсной сетки и передачи сигнала в эфир.

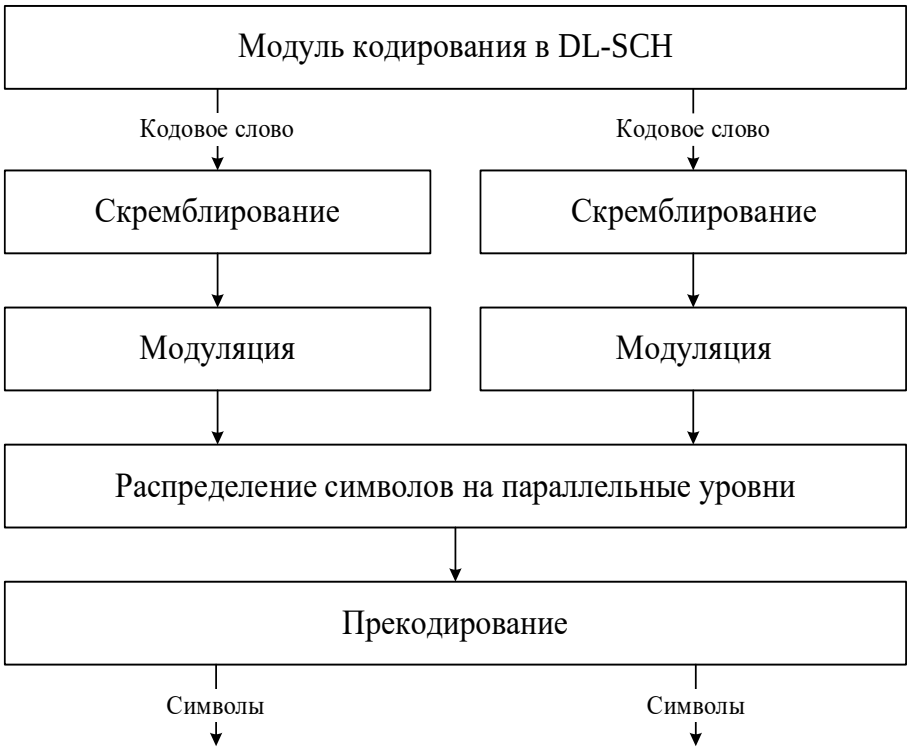

Рисунок 4

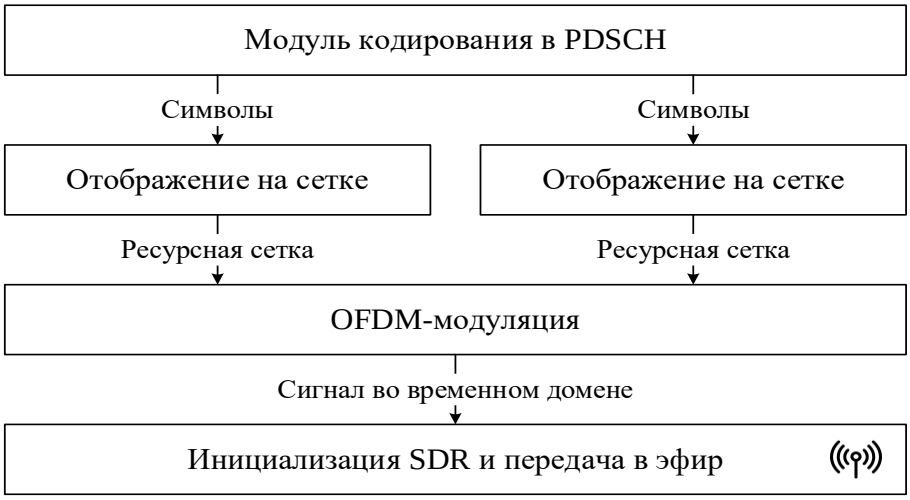

Рисунок 5

Процедуры приема навигационных данных

На приемной стороне выполняются обратные процедуры, из которых итоговой является вывод местоположения макета базовой станции *eNB* на карте в глобальной СК *WGS*-84.

Рисунок 6 иллюстрирует обобщенную последовательность процедур приема и декодирования навигационных данных.

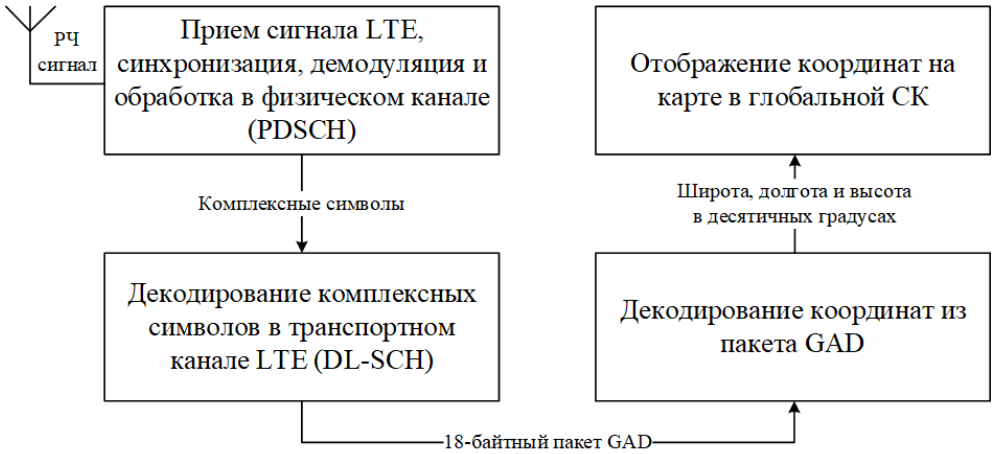

Рисунок 6

Процедуры приема и обработки в физическом канале *LTE*

Перед декодированием физического канала *PDSCH* выполняются следующие процедуры: 1) инициализация *SDR*-платформы и запись сигнала из эфира; 2) оценка и коррекция частотного сдвига; 3) вычисление корреляций по *PSS* и *SSS* для определения границ кадра и обнаружения идентификатора соты *Cell ID*; 4) демодуляция *OFDM*-сигнала; 5) извлечение комплексных символов навигационных данных из ресурсной сетки в соответствии с *Cell ID*.

Рисунок 7 иллюстрирует диаграмму последовательности процедур приема и извлечения символов навигационных данных.

После получения из эфира комплексных символов навигационных данных они обрабатываются в физическом канале *PDSCH* согласно следующим

процедурам: 1) депрекодирование; 2) извлечение символов из параллельных уровней; 3) демодуляция символов; 4) дескремблирование.

Рисунок 8 иллюстрирует диаграмму последовательности процедур обработки в физическом канале *PDSCH* на стороне приемника.

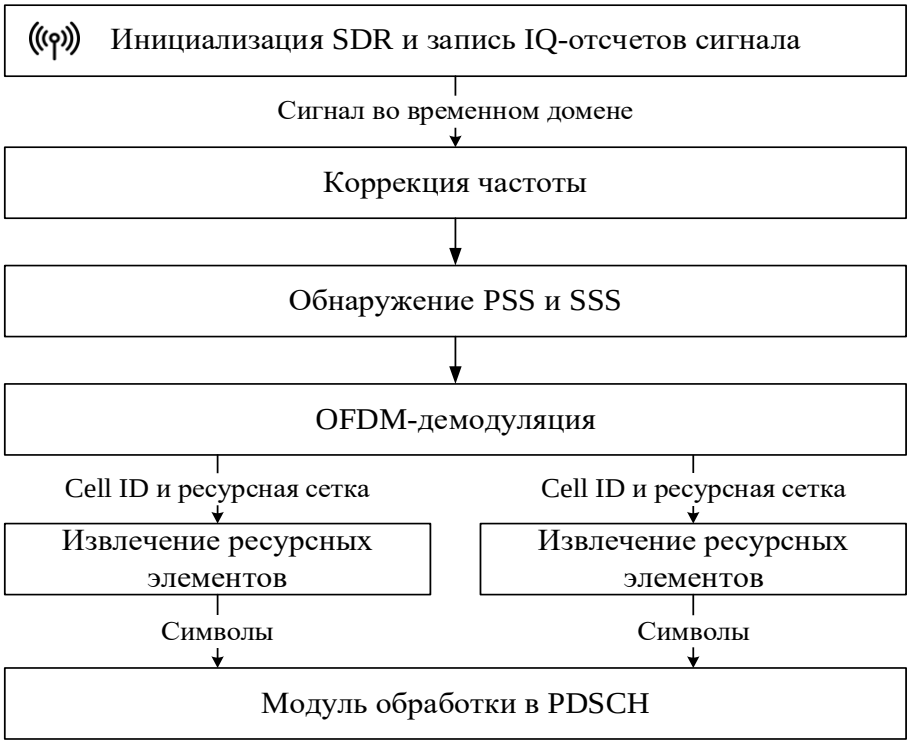

Рисунок 7

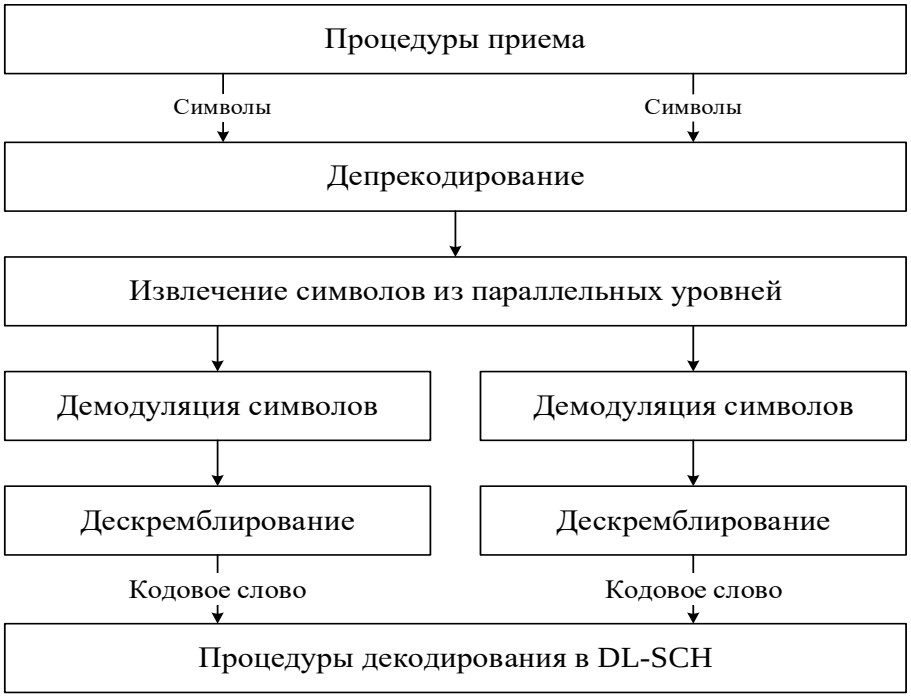

Рисунок 8

Процедуры декодирования в транспортном канале *LTE*

После обработки навигационных данных в физическом канале *PDSCH* их необходимо декодировать в транспортном канале *DL-SCH* согласно следующим процедурам: 1) разделение на кодовые блоки; 2) восстановление скорости; 3) помехоустойчивое канальное турбо-декодирование; 4) объединение кодовых блоков; 5) вычисление и проверка контрольной суммы.

Рисунок 9 иллюстрирует диаграмму последовательности процедур декодирования навигационных данных в транспортном канале *DL-SCH*.

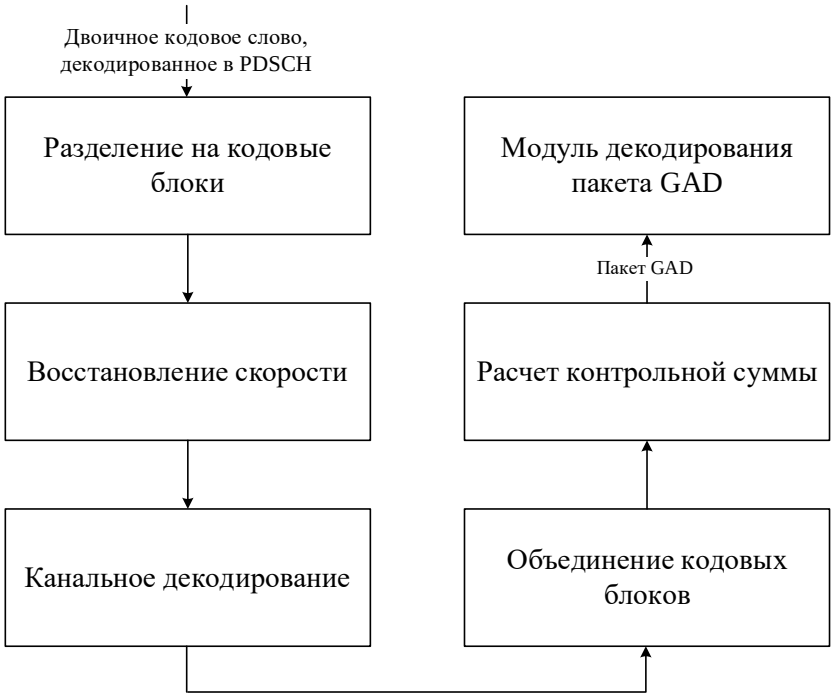

Рисунок 9

Процедуры декодирования навигационных данных из пакета *GAD*

Поля пакета навигационных данных, полученные после декодирования в транспортном канале *DL-SCH*, поочередно преобразуются из двоичного представления в десятичные кодовые числа, а затем в значения широты, долготы и высоты в соответствии с [24]. Далее эти координаты отображаются в виде точки на карте в глобальной СК.

Экспериментальная апробация

Экспериментальная апробация приемопередатчика навигационных данных в сети *LTE* проводилась с использованием *SDR*-платформы *USRP B*210 [25] и ГНСС-приемника *Globalsat BU*-353S4 [26] и заключалась в приеме глобальных координат ГНСС-приемником на стороне макета *eNB*, кодировании их, передаче в эфир, приеме *LTE* сигнала макетом *UE*, декодировании навигационных данных и отображении на карте местоположения макета *eNB* в соответствии с вышеописанными процедурами. Фото экспериментального стенда приведено на рис. 10. Слева на рис. 10 располагается макет *eNB*, а справа – макет *UE*.

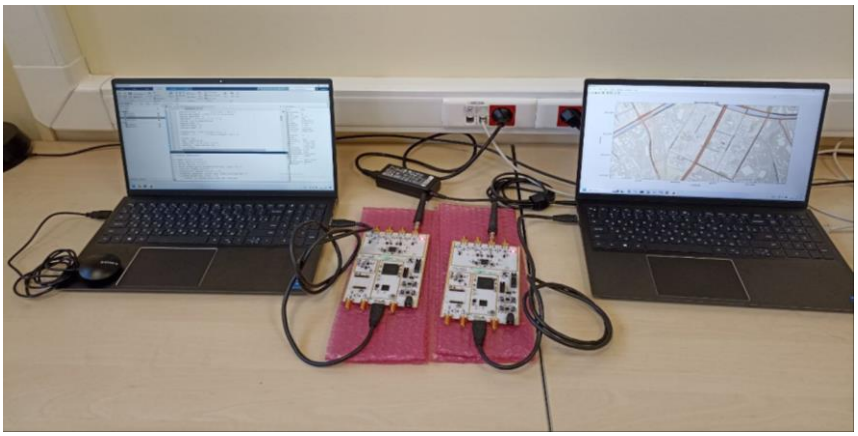

Рисунок 10

На стороне передатчика в командном окне *MATLAB* выводится информация о зафиксированных ГНСС-приемником навигационных данных (рисунок 11). На стороне приемника макета *UE* после успешной демодуляции и декодирования выводится графическое окно с картой в глобальной СК и отображенным на ней местоположением макета *eNB* (рисунок 12).

```
Command Window
Координаты зафиксированы!

1) Время (UTS+3): 12:04:09
2) Широта (WGS-48): 59.9106 N
3) Долгота (WGS-48): 30.35 E
6) Высота антенны над/под средним уровнем моря (геоид): 38.8 M
4) Количество видимых спутников: 12
5) Горизонтальное снижение точности: 0.8
7) Геоидальное разделение, разница между земным эллипсоидом WGS-84
   и средним уровнем моря (геоид): 18 M
   '-' означает, что средний уровень моря ниже эллипсоида
```

Рисунок 11

Рисунок 12

В ходе экспериментальной апробации приемопередатчика навигационных данных в сети стандарта *LTE* были успешно переданы, приняты и декодированы глобальные координаты *SDR*-макета *eNB.*

Заключение

В результате проведенного исследования был разработан и экспериментально апробирован приемопередатчик навигационных данных в сети стандарта *LTE*. Реализация описанных процедур кодирования и декодирования позволяет использовать его для приема и передачи не только навигационных, но и любых других данных. Направлением дальнейших исследований является реализация разработанных алгоритмов на ПЛИС (программируемая логическая интегральная схема).

Литература

1. Koelemeij J.C.J., Dun H., Diouf C.E.V. [et al] A hybrid optical-wireless network for decimetre-level terrestrial positioning // Nature, 2022. – Vol. 611. – № 7936. – P. 473-478.
2. Diouf C., Janssen G.J.M., Dun H., Kazaz T., Tiberius C.C.J.M. A USRP-Based Testbed for Wideband Ranging and Positioning Signal Acquisition // in IEEE Transactions on Instrumentation and Measurement, 2021. – Vol. 70. – P. 1-15.
3. Yan H., Hanna S., Balke K., Gupta R., Cabric D., Software Defined Radio Implementation of Carrier and Timing Synchronization for Distributed Arrays // 2019 IEEE Aerospace Conference, Big Sky. – MT, USA, 2019. – P. 1-12.
4. Diouf C., Janssen G.J.M., Kazaz T., Dun H., Chamanzadeh F., Tiberius C.C.J.M. A 400 Msps SDR platform for prototyping accurate wideband ranging techniques // 2019 16th Workshop on Positioning, Navigation and Communications (WPNC). – Bremen, Germany, 2019. – P. 1-6.
5. Prager S., Haynes M.S., Moghaddam M. Wireless Subnanosecond RF Synchronization for Distributed Ultrawideband Software-Defined Radar Networks // in IEEE Transactions on Microwave Theory and Techniques, 2020. – Vol. 68. – № 11. – P. 4787-4804.
6. Prager S., Thrivikraman T., Haynes M., Stang J., Hawkins D., Moghaddam M. Ultra-wideband synthesis for high-range resolution software defined radar // 2018 IEEE Radar Conference (RadarConf18). - Oklahoma City, OK, USA, 2018. – P. 1089-1094.
7. Dun H., Tiberius C.C.J.M., Diouf C., Janssen G.J.M. Terrestrial Precise Positioning System Using Carrier Phase from Burst Signals and Optically Distributed Time and Frequency Reference // Proceedings of the 2021 International Technical Meeting of The Institute of Navigation, 2021. – P. 510-524.
8. Peral-Rosado J. A. [et al] Software-defined radio LTE positioning receiver towards future hybrid localization systems // in Proceedings of 31st AIAA International Communications Satellite Systems Conference, 2013. – P. 5610.
9. Driusso M., Marshall C., Sabathy M., Knutti F., Mathis H., Babich F. Vehicular Position Tracking Using LTE Signals // in IEEE Transactions on Vehicular Technology, 2017. – Vol. 66. – № 4. – P. 3376-3391.
10. Driusso M., Babich F., Knutti F., Sabathy M., Marshall C. Estimation and tracking of LTE signals time of arrival in a mobile multipath environment // 2015 9th International Symposium on Image and Signal Processing and Analysis (ISPA). – Zagreb, Croatia, 2015. – P. 276-281.
11. Fokin G., Volgushev D. Software-Defined Radio Network Positioning Technology Design. Problem Statement // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications. – Moscow, Russian Federation, 2022. – P. 1-6.

12. Fokin G., Volgushev D. Software-Defined Radio Network Positioning Technology Design. Transmitter Development // 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). – Sofia, Bulgaria, 2022. – P. 153-158.
13. Volgushev D., Fokin G. Software-Defined Radio Network Positioning Technology Design. Receiver Development // 2022 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED). – Moscow, Russian Federation, 2022. – P. 1-6.
14. Fokin G., Volgushev D. Software-Defined Radio Network Positioning Technology Design. Receiver Processing Procedures // 2023 Systems of Signals Generating and Processing in the Field of on Board Communications. – Moscow, Russian Federation, 2023. – P. 1-7.
15. Fokin G., Ryutin K., Grigoriev V., Bobrovskiy V. Software-Defined Radio Network Positioning Technology Design. Synchronization Subsystem // 2023 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). - Pskov, Russian Federation, 2023. – P. 1-6.
16. Fokin G., Volgushev D., Grigoriev V., Ryutin K. Software-Defined Radio Network Positioning Technology Design. Field Experiment Demonstrator // 2023 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED). – Moscow, Russian Federation, 2023. – P. 1-6.
17. Ryutin K.E., Fokin G.A. Software-Defined Radio Network Positioning Technology Design. MIB Transceiver Development // 2023 Seminar on Signal Processing. – Saint Petersburg, Russian Federation, 2023. – P. 115-119.
18. Mashkov G., Borisov E., Fokin G. Experimental validation of multipoint joint processing of range measurements via software-defined radio testbed // 2017 19th International Conference on Advanced Communication Technology (ICACT). – PyeongChang, Korea (South), 2017. – P. 979-984.
19. Mashkov G., Borisov E., Fokin G. Positioning accuracy experimental evaluation in SDR-based MLAT with joint processing of range measurements // 2016 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET). - Jakarta, Indonesia, 2016. – P. 7-12.
20. Mashkov G., Borisov E., Fokin G. Experimental validation of multipoint joint processing of range measurements via software-defined radio testbed // 2016 18th International Conference on Advanced Communication Technology (ICACT). - PyeongChang, Korea (South), 2016. – P. 268-273.
21. 3GPP TS 36.214 V17.0.0 (2022-03) Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer; Measurements (Release 17).
22. 3GPP TS 38.215 V18.1.0 (2023-12) NR; Physical layer measurements (Release 18).
23. NMEA 0183-Standard for interfacing marine electronic devices: Version 3.01.2002.
24. 3GPP TS 23.032. Universal Geographical Area Description (GAD). V17.2.0, 2021-12.
25. URL https://www.ettus.com/all-products/ub210-kit/ (дата обращения – март 2024 г.).
26. URL https://www.globalsat.ru/catalog/snyatye/bu-353s4 (дата обращения – март 2024 г.).

ИССЛЕДОВАНИЕ ИМПУЛЬСНОГО ЛЧМ СИГНАЛА С НЕПРЯМОУГОЛЬНОЙ ОГИБАЮЩЕЙ

Д.А. Везарко, *Московский технический университет связи и информатики, vezarko00@mail.ru;*
А.С. Чечельницкий, *Московский технический университет связи и информатики, mr.vip64@yandex.ru;*
В.А. Коптев, *Московский технический университет связи и информатики, yyy.xxx.98@bk.ru;*
Б.М. Халматов, *Московский технический университет связи и информатики, wotblitzdrd@gmail.com.*

УДК 621.396.96

Аннотация. Проводится комплексное исследование потенциальных возможностей измерения дальности и частоты доплера для импульсного сигнала с внутриимпульсной частотной линейной модуляцией и непрямоугольной огибающей при неизвестной начальной фазе. С помощью среды моделирования *MatLab* производится вычисление основных параметров, а также построение информативных характеристик сигнала.

Ключевые слова: линейная частотная модуляция (ЛЧМ); радиолокация; комплексная огибающая; функция неопределенности (ФН); автокорреляционная функция (АКФ); частотно-корреляционная функция (ЧКФ); задержка; допплеровский сдвиг; точность оценивания; совместное оценивание; неизвестная начальная фаза.

INVESTIGATION OF A PULSE LFM SIGNAL WITH A NON-RECTANGULAR ENVELOPE

Daniil Vezarko, *Moscow Technical University of Communications and Informatics;*
Alexei Chechelnitsky, *Moscow Technical University of Communications and Informatics;*
Viktor Koptev, *Moscow Technical University of Communications and Informatics;*
Bogdan Khalmatov, *Moscow Technical University of Communications and Informatics.*

Annotation. A comprehensive study of the potential capabilities for measuring range and doppler frequency for a pulse signal with intra-pulse linear frequency modulation and a non-rectangular envelope with an unknown initial phase is conducted. Using the *MATLAB* simulation environment, the main parameters are calculated, and informative characteristics of the signal are constructed.

Keywords: linear frequency modulation (*LFM*); radar; complex envelope; ambiguity function (*AF*); autocorrelation function (*ACF*); frequency-correlation function (*FCF*); delay; doppler shift; estimation accuracy; joint estimation; unknown initial phase.

Введение

В настоящее время в радиотехнике, в частности в радиолокации, широкое применение находят сложные сигналы.

В радиолокаторах боевого режима применяются импульсные сигналы с невысокой пиковой мощностью, но большой базой для создания необходимого энергетического потенциала и обеспечения скрытности работы радиолокационной станции [1]. Кроме того, для задачи обнаружения низколетящих малоразмерных летательных аппаратов требуется обеспечение малого импульсного объема радиолокационной станции, что достигается путем выбора оптимального

зондирующего сигнала (ЗС), имеющего хорошую разрешающую способность по дальности и достаточно низкий уровень боковых лепестков функции селекции по дальности [2, 3].

Актуальным в этом плане является использование импульсного ЛЧМ сигнала. Такой сигнал достаточно прост в аппаратной реализации, при этом обладает весьма полезными свойствами: может обеспечить достаточно высокую разрешающую способность по дальности без сокращения длительности зондирующих импульсов. Способен создать высокую среднюю мощность ЗС, а следовательно, большую дальность обнаружения целей.

Обыкновенный ЛЧМ сигнал можно модифицировать, используя амплитудную модуляцию (т.е. синтезировав ЛЧМ сигнал с непрямоугольной огибающей). Такая модификация позволяет улучшить форму ФН, значительно уменьшить уровень боковых лепестков по скорости и дальности.

В литературе широко описаны достоинства ЛЧМ сигнала с гауссовой, огибающей [4, 5]. В работе, однако, огибающая ЛЧМ сигнала задана в виде функции $cos^2()$. Расчет и построение всех графических зависимостей производится по цифровому эквиваленту комплексной огибающей сигнала.

Одним из основных критериев при выборе ЗС является потенциальная точность оценивания ключевых параметров сигнала для задач радиолокации, а именно: доплеровского сдвига и задержки.

Приводятся основные соотношения и графические зависимости среднеквадратического отклонения (СКО) оцениваемого параметра от отношения сигнал/шум (ОСШ) при неизвестной начальной фазе.

Математическая модель сигнала и теоретическое описание исследования

Исследуемые алгоритмы отражают несколько основных шагов, которые будут описаны ниже. Ниже приведена общая последовательность, которая предполагает использование углового алгоритма распознавания:

Исследуемый в работе сигнал задан с помощью комплексной огибающей. Комплексная огибающая является универсальным и однозначным способом описания большого класса сложных сигналов, позволяет описать закон амплитудной и фазовой (частотной) модуляции сигнала. В общем виде комплексная огибающая описывается выражением (1):

$$\dot{x}_0(t) = |\dot{x}_0(t)|e^{j\gamma(t)}, \quad (1)$$

где: $|\dot{x}_0(t)|$ – модуль комплексной огибающей или тип огибающей, описывает закон амплитудной модуляции сигнала; $\gamma(t)$ – фаза комплексной огибающей или тип модулирующей функции, описывает закон внутриимпульсной модуляции сигнала.

Модуль комплексной огибающей $|\dot{x}_0(t)|$ для исследуемого сигнала задан в виде функции (2):

$$|\dot{x}_0(t)| = cos^2\left(\pi\frac{t}{T_s}\right), -\frac{T_s}{2} < t \leq \frac{T_s}{2} \quad (2)$$

где: T_s – длительность сигнала, при моделировании составляет 0,5 мкс.

Функция, описывающая закон изменения мгновенной частоты сигнала внутри длительности импульса, имеет следующий вид (3):

$$f_s(t) = f_1 + \frac{1}{T_s}(f_2 - f_1)\left(t + \frac{T_s}{2}\right), -\frac{T_s}{2} < t \leq \frac{T_s}{2} \quad (3)$$

где: $f_1 = -40$ МГц; $f_2 = 40$ МГц – значения граничных частот линейного закона изменения мгновенной частоты. Девиация частоты ЛЧМ сигнала при моделировании составляет $\Delta f = |f_2 - f_1| = 80$ МГц.

При этом функция, описывающая закон изменения фазы комплексной огибающей, является интегралом от выражения (3) и представляется в следующем виде:

$$\begin{gathered}\gamma(t) = 2\pi \int_{-\frac{T_s}{2}}^{t} f_s(t)dt = 2\pi f_1 t + \\ + \frac{2\pi}{2T_s}(f_2 - f_1)(t^2 + T_s t) + \\ + 2\pi\left[\frac{f_1 T_s}{2} + \frac{1}{8}(f_2 - f_1)T_s\right], -\frac{T_s}{2} < t \leq \frac{T_s}{2}\end{gathered} \quad (4)$$

Для оценки совместной разрешающей способности ЗС по дальности и скорости применяется ФН. В работе рассчитывается ФН радиолокационного сигнала, приводится трехмерное изображение тела ФН, анализируются важные сечения – АКФ и ЧКФ.

По определению ФН задается выражением (5):

$$|\Psi(\tau, f_d)| = \left| \int_{-\infty}^{\infty} \dot{x}_0(t) \cdot \dot{x}_0^*(t - \tau) e^{j2\pi f_d t} dt \right|, \quad (5)$$

где: $\dot{x}_0^*(t - \tau)$ – функция, которая является комплексно-сопряженной к комплексной огибающей сигнала, τ – задержка сигнала, f_d – доплеровский сдвиг.

Таким образом, ФН представляет из себя объем над плоскостью (τ, f_d) и состоит из главного максимума при $\tau = 0$, f_d=0 и ряда побочных, меньшей высоты [6].

Данная функция показывает относительную степень отклика согласованного фильтра (СФ) на сигнал, задержанный по времени на τ и по частоте на *F* относительно сигнала, оптимального в этом устройстве. Другими словами, ФН характеризует степень различия откликов устройств на указанные типы сигналов. Количественно позволяет оценить разрешающую способность по времени и частоте.

Для более наглядного представления о разрешающей способности по времени и частоте в исходном выражении (5) попеременно полагают $\tau = 0$ и f_d=0. Функция $|\Psi(0, f_d)| = |\Psi(f_d)|$ является сечением ФН вертикальной плоскостью при $\tau = 0$ (носит название АКФ), ширина такого сечения будет определять разрешающую способность по частоте и точность измерения скорости движения целей. Функция $|\Psi(\tau, 0)| = |\Psi(\tau)|$ является сечением ФН вертикальной плоскостью при f_d=0 (носит название ЧКФ). Ширина такого сечения определяет разрешающую способность по задержке и точность измерения дальности [7].

В радиолокации задача оценивания параметров сигнала ставится из необходимости получения информации о координатах или скорости движения цели. Любая радиотехническая система неидеальна, параметры сигнала подвержены действию случайных факторов, под которыми понимаются все

сторонние возмущения, приводящие к искажению сигнала. Поэтому оценка параметров сигнала реализуется с помощью статистических методов.

Оцениваемые параметры можно разделить на два класса: энергетические и неэнергетические. В работе рассматривается потенциальная точность совместной оценки исключительно неэнергетических параметров, а именно: задержки сигнала и доплеровского сдвига, начальная фаза полагается неизвестной.

Для неэнергетических параметров ОСШ на выходе оптимального приемника не зависит от конкретного значения оцениваемого параметра.

Теория, по части совместной оценки нескольких параметров, является обобщением результатов, полученных для оценки единственного параметра сигнала и подробно изложена в [8].

В работе за основной показатель качества принята дисперсия оценки. Выражения для соответствующих дисперсий приводятся ниже.

Для дисперсии оценки задержки $\tilde{\tau}$ при оценивании только задержки при неизвестной начальной фазе φ (без оценивания доплеровского сдвига) существует выражение (6):

$$D(\tilde{\tau}\ /\varphi) = \frac{1}{4\pi^2\rho^2 F_{\text{эфф}}^2}, \tag{6}$$

где: $\rho^2 = \frac{2E_s}{N_0}$ – ОСШ на выходе СФ, E_s – энергия сигнала, N_0 – энергия шума, $F_{\text{эфф}} = \sqrt{\frac{\int_{-\infty}^{\infty}(f-f_0)^2|\dot{X}(j2\pi f)|^2 df}{\int_{-\infty}^{\infty}|\dot{X}(j2\pi f)|^2 df}}$ – среднеквадратическая ширина спектра сигнала, $f_0 = \frac{\int_{-\infty}^{\infty} f\,|\dot{X}(j2\pi f)|^2 df}{\int_{-\infty}^{\infty}|\dot{X}(j2\pi f)|^2 df}$ – центр масс спектральной плотности мощности сигнала, $|\dot{X}(j2\pi f)|$ – спектральная плотность мощности сигнала.

Для дисперсии оценки доплеровского сдвига $\tilde{f}_d$ при оценивании только доплеровского сдвига при неизвестной начальной фазе φ (без оценивания задержки) существует выражение (7):

$$D(\tilde{f}_d\ /\varphi) = \frac{1}{4\pi^2\rho^2 T_{\text{эфф}}^2}, \tag{7}$$

где: $T_{\text{эфф}} = \sqrt{\frac{\int_{-\infty}^{\infty}(t-\tau_0)^2|\dot{x}_0(t)|^2 dt}{\int_{-\infty}^{\infty}|\dot{x}_0(t)|^2 dt}}$ – среднеквадратическая длительность сигнала, $\tau_0 = \frac{\int_{-\infty}^{\infty} t|\dot{x}_0(t)|^2 dt}{\int_{-\infty}^{\infty}|\dot{x}_0(t)|^2 dt}$ – центр масс мгновенной мощности сигнала.

Для дисперсии оценки задержки $\tilde{\tau}$ при совместном оценивании параметров (с неизвестной начальной фазой φ) существует выражение (8):

$$D(\tilde{\tau}/\varphi, f_d) = \frac{1}{4\pi^2\rho^2 F_{\text{эфф}}^2(1-\rho_{\tau f}^2)}, \tag{8}$$

где: $\rho_{\tau f} = \frac{\int_{-\infty}^{\infty} t f_s(t)|\dot{x}_0(t)|^2 dt}{T_{\text{эфф}}F_{\text{эфф}}\int_{-\infty}^{\infty}|\dot{x}_0(t)|^2 dt}$ – коэффициент частотно-временной связи (для исследуемого сигнала близок к 1).

Для дисперсии оценки доплеровского сдвига $\tilde{f}_d$ при совместном оценивании параметров (с неизвестной начальной фазой φ) существует выражение (9):

$$D(\tilde{f}_d/\varphi,\tau)=\frac{1}{4\pi^2\rho^2T_{\text{эфф}}^2(1-\rho_{\tau f}^2)}, \quad (9)$$

Одним из результатов работы будет построение зависимостей СКО (корень из дисперсии) от ОСШ задержки и доплеровского сдвига при неизвестной начальной фазе, а также оценки задержки (без оценивания доплеровского сдвига) и оценки доплеровского сдвига (без оценивания задержки) при неизвестной начальной фазе сигнала.

Моделирование сигнала и расчет характеристик на ЭВМ

Исследование выполняется с помощью программной среды моделирования *MatLab*.

Как уже описывалось ранее, сигнал задается с помощью своей комплексной огибающей. Однако, выражение (1) описывает аналоговый сигнал. Моделирование же производится на ЭВМ, т.е. необходимо выполнить операции дискретизации по времени и квантования по уровню. Эффект квантования в работе не берется во внимание (предполагается, что разрядная сетка ЭВМ достаточно велика). Эффект дискретизации по времени, наоборот, имеет принципиальное значение и ему следует уделить особое внимание.

Необходимо правильно задать частоту дискретизации F_s. Частота дискретизации для ЛЧМ сигнала обычно задается с помощью выражения $F_s = 4\Delta f = 4 \cdot 80 = 320$ МГц.

Таким образом, удалось сформировать массив значений сигнала в *MatLab* (вектор из 640 комплексных чисел) в диапазоне от $-2T_s$ до $2T_s - 1$ с шагом $T = \frac{1}{F_s}$.

С помощью выражения (3) рассчитан и построен закон изменения во времени мгновенной частоты сигнала $f_s(t)$. Соответствующий график представлен на рис. 1.

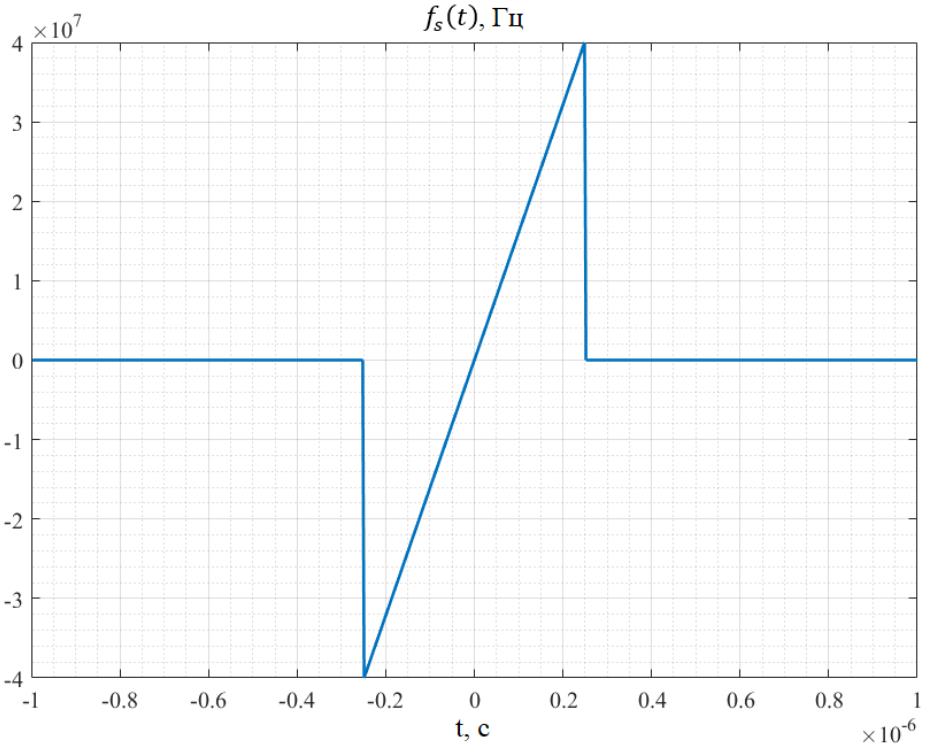

Рисунок 1

Из рис. 1 видно, что зависимость мгновенной частоты от времени $f_s(t)$ за время длительности импульса T_s носит линейно нарастающий характер, как и положено ЛЧМ сигналу.

С помощью эквивалента комплексной огибающей и выражений (2), (4), а также встроенных функций *MatLab abs*() и *angle*(), были рассчитаны и построены модуль $|\dot{x}_0(t)|$ и фаза $\gamma(t)$. Соответствующие графические зависимости приведены на рис. 2.

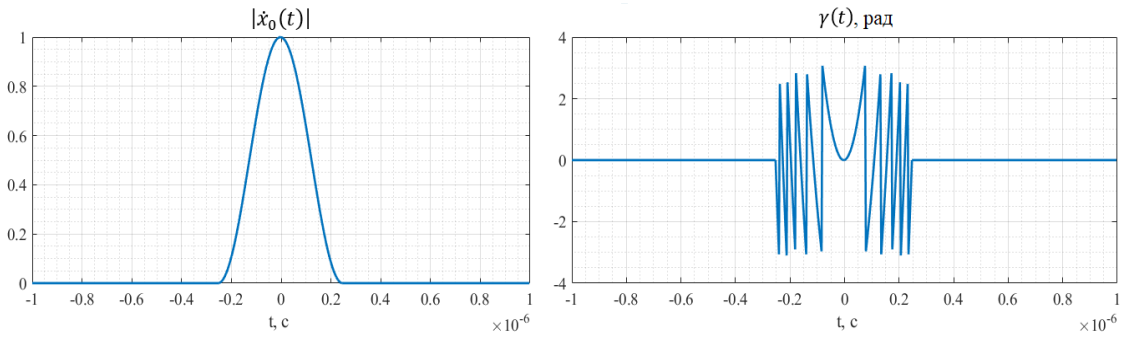

Рисунок 2

Графические зависимости, представленные на рис. 2, однозначным образом описывают исследуемый сигнал. Модуль $|\dot{x}_0(t)|$ определяет длину вектора на комплексной плоскости (имеет вид функции $cos^2()$), а фаза $\gamma(t)$ определяет скорость вращения вектора против часовой стрелки (имеет вид квадратичной функции, так как в данном случае фаза есть интеграл от функции мгновенной частоты $f_s(t)$).

С помощью встроенных функций *fft*() и *abs*() был произведен расчет амплитудного спектра сигнала. На рис. 3 представлен соответствующий график частотной зависимости амплитуды.

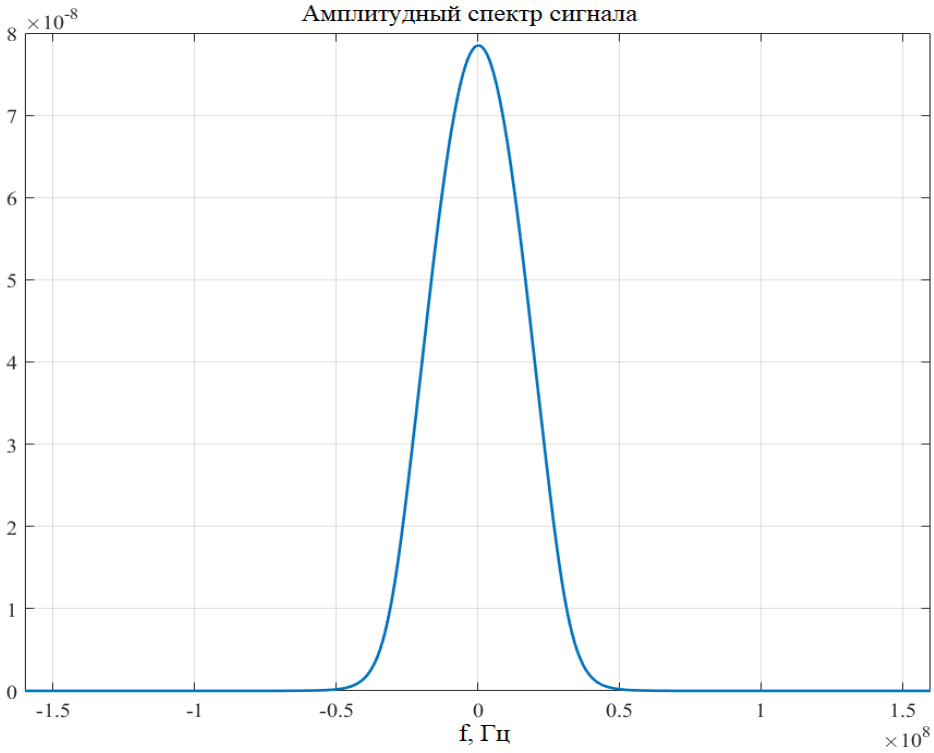

Рисунок 3

Из рис. 3 можно видеть, что ширина спектра сигнала как раз составляет порядка 80 МГц. Также можно заметить, что форма спектра значительно отличается от формы спектра классического импульсного ЛЧМ сигнала с прямоугольной огибающей, ее можно характеризовать как более сосредоточенную (большая часть энергии сигнала сосредоточена в главном лепестке).

На основе массива комплексных чисел и встроенной функции *ambgfun*(), было выполнено построение тела ФН и важные сечения этой функции (АКФ, ЧКФ, а также сечения по уровню). Соответствующие графические зависимости представлены ниже на рис. 4 и 5.

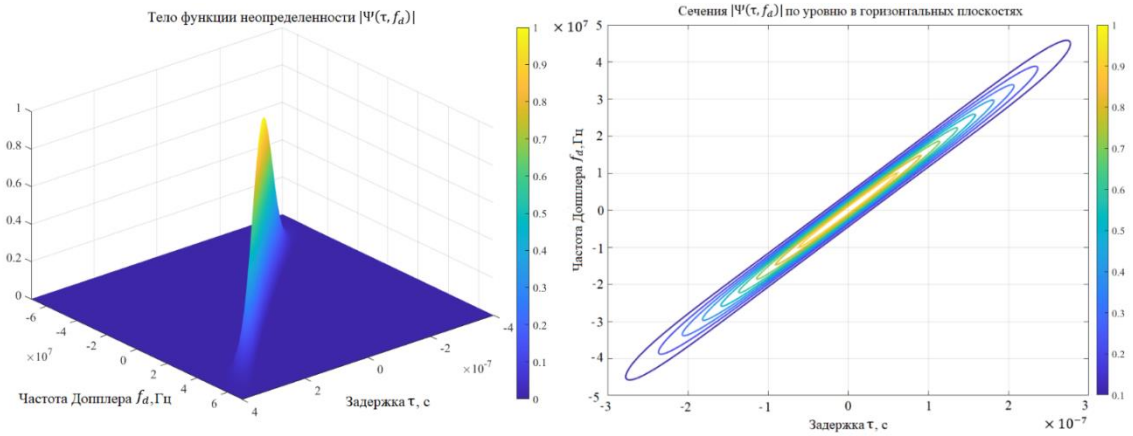

Рисунок 4

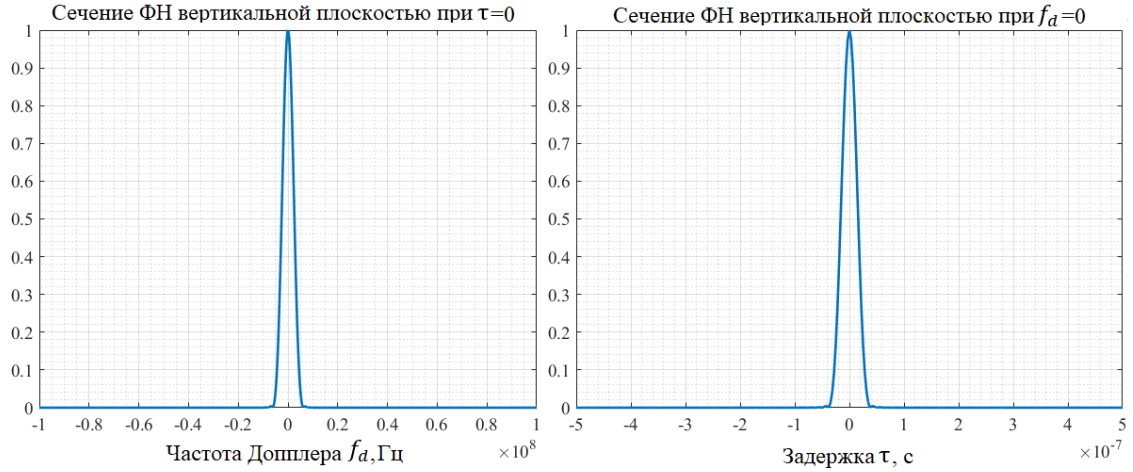

Рисунок 5

Исходя из рис. 4 и 5 видно, что тело ФН исследуемого сигнала имеет «ножевидную» форму, как и для классического ЛЧМ сигнала [6]. Однако, уровень побочных максимумов для сигнала с огибающей вида $cos^2()$ гораздо более низкий (в линейном масштабе соседние лепестки практически не заметны).

Для исследуемого типа ЗС с заданными параметрами разрешающая способность составила:

- ~ 5 МГц по частоте Допплера;
- ~ 5 м по дальности.

С помощью соотношений (6), (7), (8) и (9) для нижних границ дисперсий оценок рассчитаны и построены графики зависимостей среднеквадратического отклонения от ОСШ для: $\sqrt{D(\tilde{\tau}\ /\varphi)}$, $\sqrt{D(\tilde{\tau}/\varphi, f_d)}$, $\sqrt{D(\tilde{f}_d\ /\varphi)}$, $\sqrt{D(\tilde{f}_d/\varphi, \tau)}$. Соответствующие зависимости представлены на рис. 6 и 7.

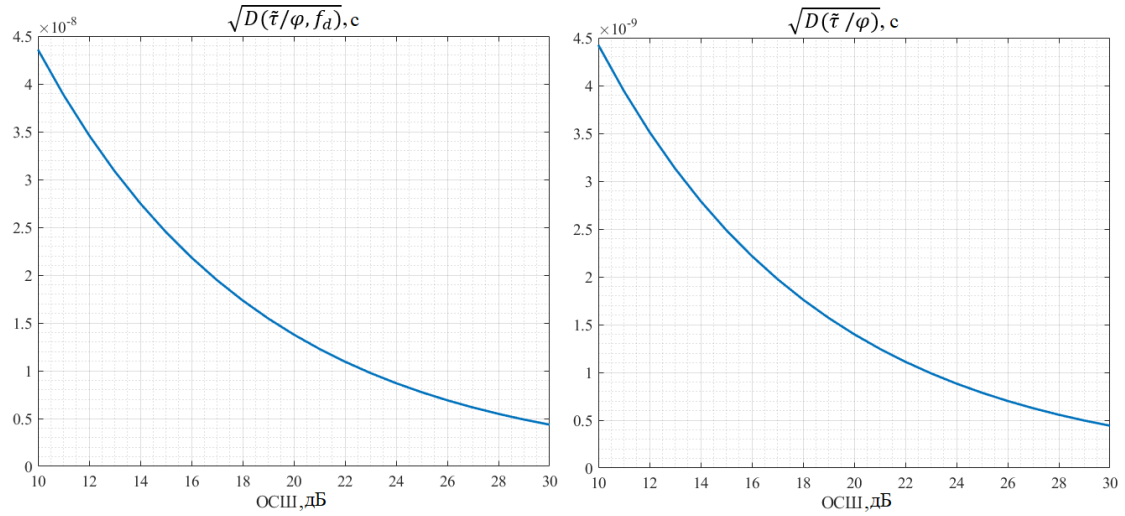

Рисунок 6

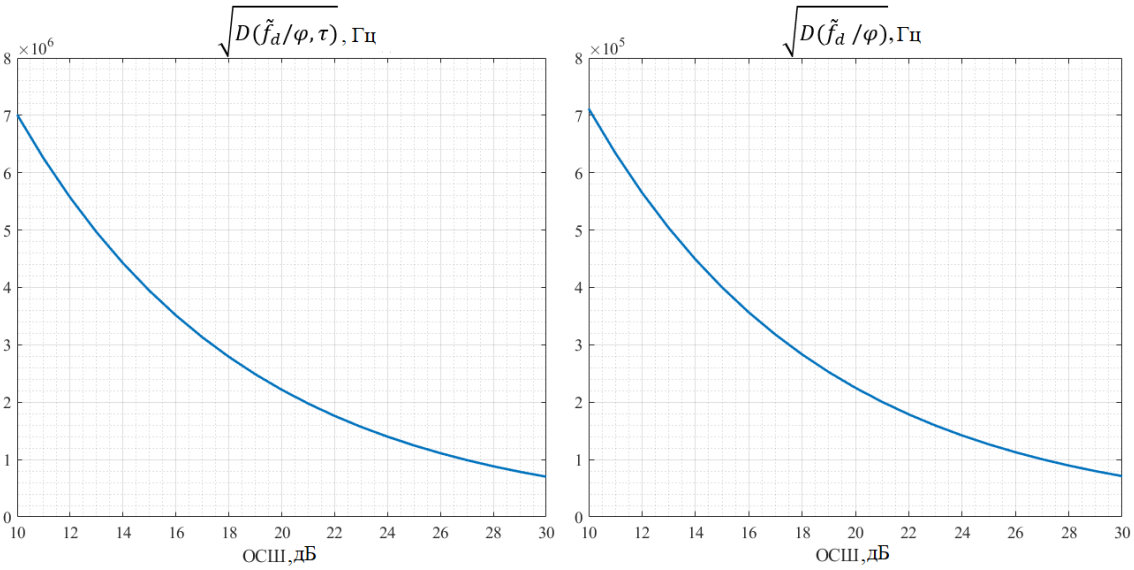

Рисунок 7

Из полученных рис. 6 и 7 можно заключить, что качество оценивания ключевых параметров сигнала (задержки и допплеровского сдвига при неизвестной начальной фазе) очень сильно зависит от того – производится ли совместная оценка параметров или же оценивается исключительно задержка τ (либо доплеровский сдвиг f_d). При совместном оценивании качество оценивания ухудшается на порядок. Такое сильное различие в качестве оценки свидетельствует о том, что для данного типа сигнала существует сильная корреляционная связь частотных и временных параметров сигнала – о чем говорит коэффициент частотно-временной связи, который для исследуемого сигнала $\rho_{\tau f} \approx 1$.

Заключение

В работе был исследован импульсный ЛЧМ сигнал с непрямоугольной огибающей. Тело ФН такого сигнала имеет «ножевидную» структуру с низким уровнем побочных максимумов. Такой сигнал имеет достаточно хорошую разрешающую способность по дальности ($\sim$ 5 м), что может обеспечить малый импульсный объем РЛС (такая особенность является полезной во многих практических приложениях радиолокации). По частоте сигнал имеет разрешение ($\sim$ 5 МГц).

Такие характеристики делают данный тип сигнала особенно подходящим для задач, требующих высокой точности измерений, например, в радиолокационных системах обнаружения или слежения за объектами.

Значение коэффициента частотно-временной связи $\rho_{\tau f} \approx 1$. Из-за этого факта сильно ухудшается совместная оценка параметров (задержка τ и доплеровский сдвиг f_d), что хорошо можно видеть из рис. 6 и 7.

Литература

1. Соколов А.В. Вопросы перспективной радиолокации // – М.: Радиотехника, 2003. – 512 с.
2. Ананенков А.Е. К вопросу о наблюдении малоразмерных беспилотных летательных аппаратов // Труды МАИ, 2016. – № 91.
3. Ананенков А.Е. Обнаружение малоразмерных объектов сверхкороткоимпульсной РЛС // Сверхширокополосные сигналы в радиолокации, связи и акустике, 2007.
4. Кук Ч., Бернфельд М. Радиолокационные сигналы. – М.: Сов. Радио, 1971. – 568 с.
5. Тисленко В.И. Статистические методы обработки сигналов в радиотехнических системах. – Томск.: Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. – 245 с.
6. Сперанский В.С. Радиолокация, радиолокационные системы и устройства. – М.: Брис-М, 2011. – 257 с.
7. Гришин Ю.П., В.П. Ипатов и др. Радиотехнические системы: Учеб. для вузов по спец. «Радиотехника». Под ред. Ю.М. Казаринова. – М.: Высш. шк. – 1990. – 496 с.
8. Куликов Е.И. Оценка параметров сигналов на фоне помех. – М.: Советское радио, 1978. – 296 с.

РАДИОЛОКАЦИОННАЯ СИСТЕМА БЛИЖНЕГО ОБНАРУЖЕНИЯ С ПРИМЕНЕНИЕМ СИГНАЛА OFDM И ЕЕ ВОЗМОЖНОСТИ ОБНАРУЖЕНИЯ СОВРЕМЕННЫХ ЦЕЛЕЙ

В.А. Коптев, *Московский технический университет связи и информатики, yyy.xxx.98@bk.ru;*
Д.А. Везарко, *Московский технический университет связи и информатики, vezarko00@mail.ru;*
Б.М. Халматов, *Московский технический университет связи и информатики, wotblitzdrd@gmail.com;*
А.С. Чечельницкий, *Московский технический университет связи и информатики, mr.vip64@yandex.ru.*

УДК 621.371, 621.396

Аннотация. В работе приведена реализация РЛС при использовании в качестве зондирующего сигнала *OFDM*. Оценены свойства и параметры целей, для отслеживания которых предназначена рассматриваемая РЛС. Объяснено применение ШП *OFDM*-сигнала. Приведен и обоснован выбор ряда параметров РЛС. Спроектирована структурная схема и объяснен приблизительный алгоритм работы локатора с *OFDM*. Определены характеристики по возможности обнаружения и оценки параметров цели.

Ключевые слова: актуальные радиолокационные цели; система ближней радиолокации; *OFDM*-сигнал; функция неопределенности; разрешающая способность.

A SHORT-RANGE RADAR SYSTEM USING THE OFDM SIGNAL AND ITS CAPABILITIES FOR DETECTING MODERN TARGETS

V.A. Koptev, *Moscow Technical University of Communications and Informatics;*
D.A. Vezarko, *Moscow Technical University of Communications and Informatics;*
B.M. Khalmatov, *Moscow Technical University of Communications and Informatics;*
A.S. Chechelnitsky, *Moscow Technical University of Communications and Informatics.*

Annotation. The paper presents the implementation of radar when using *OFDM* as a probing signal. The properties and parameters of the targets that the radar in question is designed to track are evaluated. The application of the *SHP OFDM*-signal is explained. The choice of a number of radar parameters is given and justified. A block diagram is designed and an approximate algorithm for the operation of the locator with *OFDM* is explained. The characteristics of the possibility of detecting and evaluating the parameters of the target are determined.

Keywords: current radar targets; short-range radar system; *OFDM*-signal; uncertainty function; resolution.

Введение

В настоящее время в системах передачи данных часто применяется сигнал с ортогональным частотным разделением и мультиплексированием (*OFDM*) [1]. С его помощью удается повысить скорость передачи данных за счет своей высокой спектральной эффективности. Но в радиолокации этот сигнал пока не получил своего распространения, хотя представляется перспективным для различения малозаметных объектов.

Особенности современных РЛ целей

В последнее время, беспилотные летательные аппараты (БПЛА) часто применялись для атак на объекты критически важной инфраструктуры. Также они получили широкое распространение и в гражданской сфере. Поэтому стали актуальными задачи по противодействию и борьбе с БПЛА, особенно если они применяются в особо охраняемых зонах [2, 3].

Для этого БПЛА необходимо достоверно обнаружить, установить факт его использования на контролируемой территории. Обнаруживать современные БПЛА малых геометрических размеров при помощи РЛС затруднительно. Потому что запуск таких объектов осуществляется на малой высоте, они имеют малые размеры и малую отражательную способность, непредсказуемую траекторию движения и большой динамический диапазон скоростей и высот. Однако, у БПЛА, в том числе, есть и определенные особенности, которые способствуют их обнаружению.

Обычно, БПЛА разделяют по летным параметрам: взлетная масса, дальность полета, продолжительность полета и максимальная высота полета. По этим параметрам их группируют на: малые, легкие, средние, тяжелые и смешанные. Основную проблему для обнаружения представляют малые БПЛА: взлетный вес до 25 кг, радиус действия до 10-40 км, максимальная высота 3 км и продолжительность полета до 4-х часов [4].

Одной из основных характеристик цели с точки зрения радиолокации – это эффективная площадь рассеивания (ЭПР) цели. Хоть она называется площадью и измеряется в квадратных метрах это – параметр энергетический. Он устанавливает соотношение между плотностью потока мощности, создаваемой РЛС у объекта и плотностью потока мощности у антенны РЛС, созданного вторичным излучением объекта. Иными словами, ЭПР такая фиктивная площадь изотропного излучателя, которая суммирует участки объекта, вносящие значимую долю в общую плотность потока мощности вторичного излучения, распространение которого, направленно в сторону РЛС. Если размеры неровностей объекта меньше, чем $\lambda/16$, то они никак не скажутся на электромагнитной волне – отражение будет как от ровного участка [9].

Определение ЭПР цели необходимо для расчета потенциальной возможности РЛС ее обнаружить. Этот параметр зависит от сложной формы объекта, отражающих свойств деталей, из которых состоит конструкция БПЛА (например: металлический аккумулятор, камера и диэлектрический пластиковый корпус) и меняется от угла наблюдения. Поэтому, обычно, используют среднее значение ЭПР в определенном секторе углов. Аналитически ЭПР можно рассчитать для простых геометрических фигур, а для сложных объектов – определяется опытным путем, либо моделированием [5]. Для малых БПЛА ЭПР оценивается около 0,1-0,01 м^2, а может быть и того меньше за счет использования радиопрозрачных материалов. Как показывают исследования, в дециметровом диапазоне дальность обнаружения таких БПЛА составляет, соответственно, до 9-16 км и до 0,8-2 км [2, 6]. Вариант исполнения БПЛА типа «*Switchblade*» показан на рис. 1 [7].

Рисунок 1

Описание системы РЛС

Одно из направлений развития радиолокации – это применение широкополосных (ШП) сигналов, у которых эффективная полоса спектра составляет примерно 10% от несущей частоты. Их применение обусловлено рядом преимуществ по сравнению с узкополосными сигналами, а именно: высокая разрешающая способность по расстоянию, устойчивость к пассивным помехам, относительно малое затухание в средах, скрытность работы и т.д. За счет высокой

точности определения расстояния (единицы метров) такие сигналы можно применять для обнаружения малоразмерных БПЛА [9].

Все ШП сигналы, по методу образования, можно разделить на три группы: шумоподобные, короткие видеоимпульсы и многочастотные. Шумоподобный сигнал образуется с помощью специальных генераторов шума. Короткие видеоимпульсы образуются с помощью быстрого (до единиц нс) переключения радиочастотных ключей. Многочастотные ШП сигналы образуются с помощью одновременной или последовательной генерации большого числа отдельных спектральных составляющих [8].

В свою очередь, в качестве зондирующего многочастотного ШП сигнала, можно применить сигнал *OFDM*. Он состоит из множества ортогональных поднесущих частот, что дает возможность независимо анализировать сигналы на каждой из поднесущих. В добавление к этому у *OFDM*-сигнала на каждой поднесущей можно реализовать сигнал с различной модуляцией, что повышает вариативность его применения. Также *OFDM*-сигнал за счет своей структуры устойчив к узкополосным помехам. ШП сигнал является шумоподобным, за счет чего можно обеспечить скрытность работы РЛС.

Сигнал *OFDM* формируется математическими методами при помощи алгоритмов цифровой обработки сигнала (ЦОС), таких как дискретное преобразование Фурье (ДПФ) [12], аналитическое представление:

$$\dot{U}_{OFDM}(n) = \frac{1}{N}\sum_{k=1}^{N-1} \dot{X}_k * e^{i\frac{2\pi}{N}*k*n} \qquad \dot{X}_k = \sum_{n=1}^{N-1} \dot{U}_{OFDM}(n) * e^{-i\frac{2\pi}{N}*n*k}$$

где: $x(n)$ – n-й отсчет сигнала, X_k – k-й произвольный комплексный символ модуляции, N – число поднесущих, n – номер отсчета, k – номер поднесущей.

Расстояние между поднесущими и длительность импульса устанавливается из условия ортогональности. Число отсчетов на период сигнала, обычно, устанавливается равным степени числа 2. Комплексный символы модуляции устанавливаются из входных данных. Можно подобрать их специальные комбинации, которые будут влиять на разрешающую способность сигнала во временной области. При применении сигнала *OFDM* в РЛС могут потребовать внесение незначительных структурных изменений. Например, использование усилителей, рассчитанных на высокий ПИК-фактор. Или использование производительных ПЛИС, способных быстро производить математические операции в цифровом виде.

Ориентировочные параметры РЛС

Предполагается, что рассматриваемая РЛС должна быть стационарной, но с возможностью несложного перемещения станции и быстрого развертывания. Местами установки могут быть аэропорты, крыши зданий, охранных пунктов. Соответственно, масса подобных локаторов должна быть умеренной. Варианты исполнения РЛС с подходящими масса-габаритными показателями представлены на рис. 2 [13, 14].

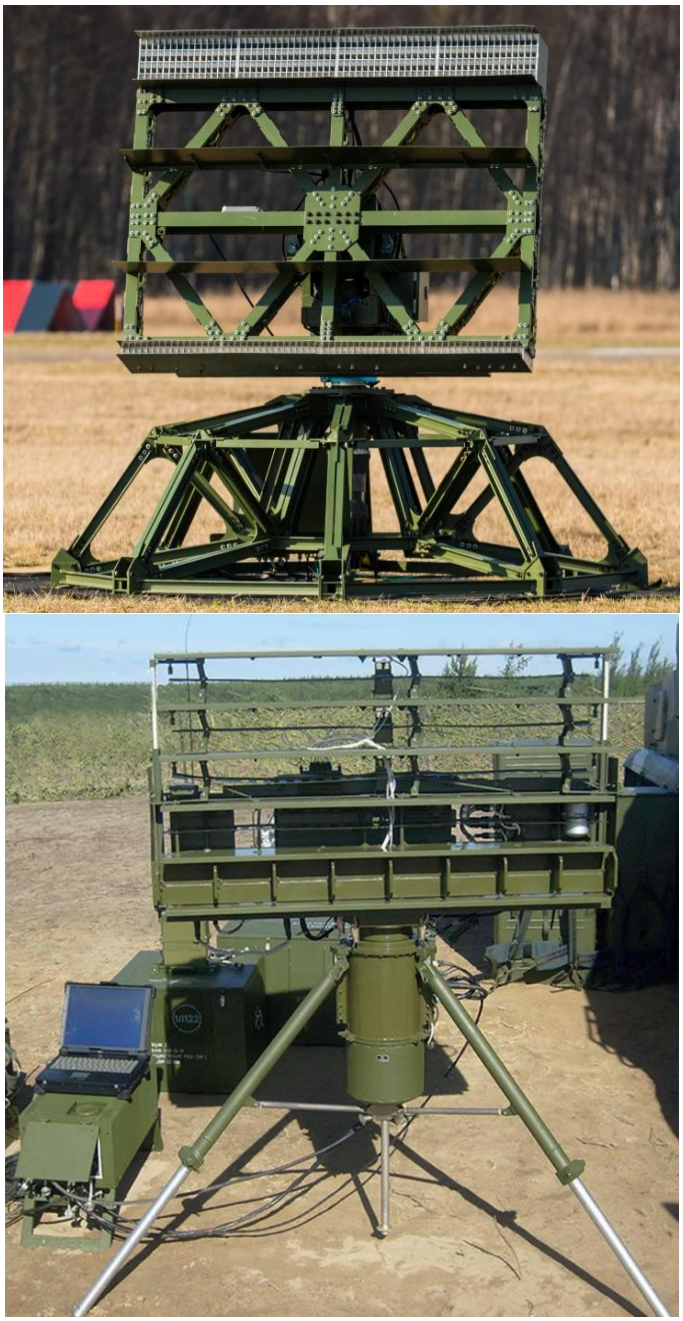

Рисунок 2

Предполагается, что частотные диапазоны работы, рассматриваемой РЛС, будут приходится на *C, X* и *Ku*, по классификации *IEEE*, то есть, соответственно, 4,0-8,0 ГГц, 8,0-12,0 ГГц и 12,0-18,0 ГГц. Работа в этих диапазонах частот обеспечивает низкий коэффициент ослабления сигнала и достаточный уровень значений определяемой ЭПР для хорошей разрешающей способности и точность определения расстояния. При этом аппаратура остается сравнительно компактной по габаритам [10, 11].

Что касается других параметров РЛС, то можно дать ориентировочные оценки. У РЛС подобного класса, обычно, выходная мощность излучения составляет сотни Ватт [13, 14]. Для удобства расчета примем, что в обычных условиях она равна 200 Вт. Предполагается, что РЛС будет использовать фазированную антенную решетку. У таких антенн коэффициент усиления составляет приблизительно 20-30 дБи [15]. Примем среднее значение коэффициента усиления антенны, он будет составлять 26 дБи.

Разработанная структурная схема РЛС

Структурная схема работы рассматриваемой РЛС представлена на рис. 3. Принцип ее работы основан на стандартных алгоритмах формирования и обработки *OFDM*-сигнала. Началом передающей части выступает блок реализации сигналов на поднесущих частотах *OFDM*. Это могут быть сигналы с квадратурно-амплитудной модуляцией или иными разнообразными видами сложных модуляций поднесущих. Блок может быть реализован с помощью генератора случайной битовой последовательности и квадратурного модулятора.

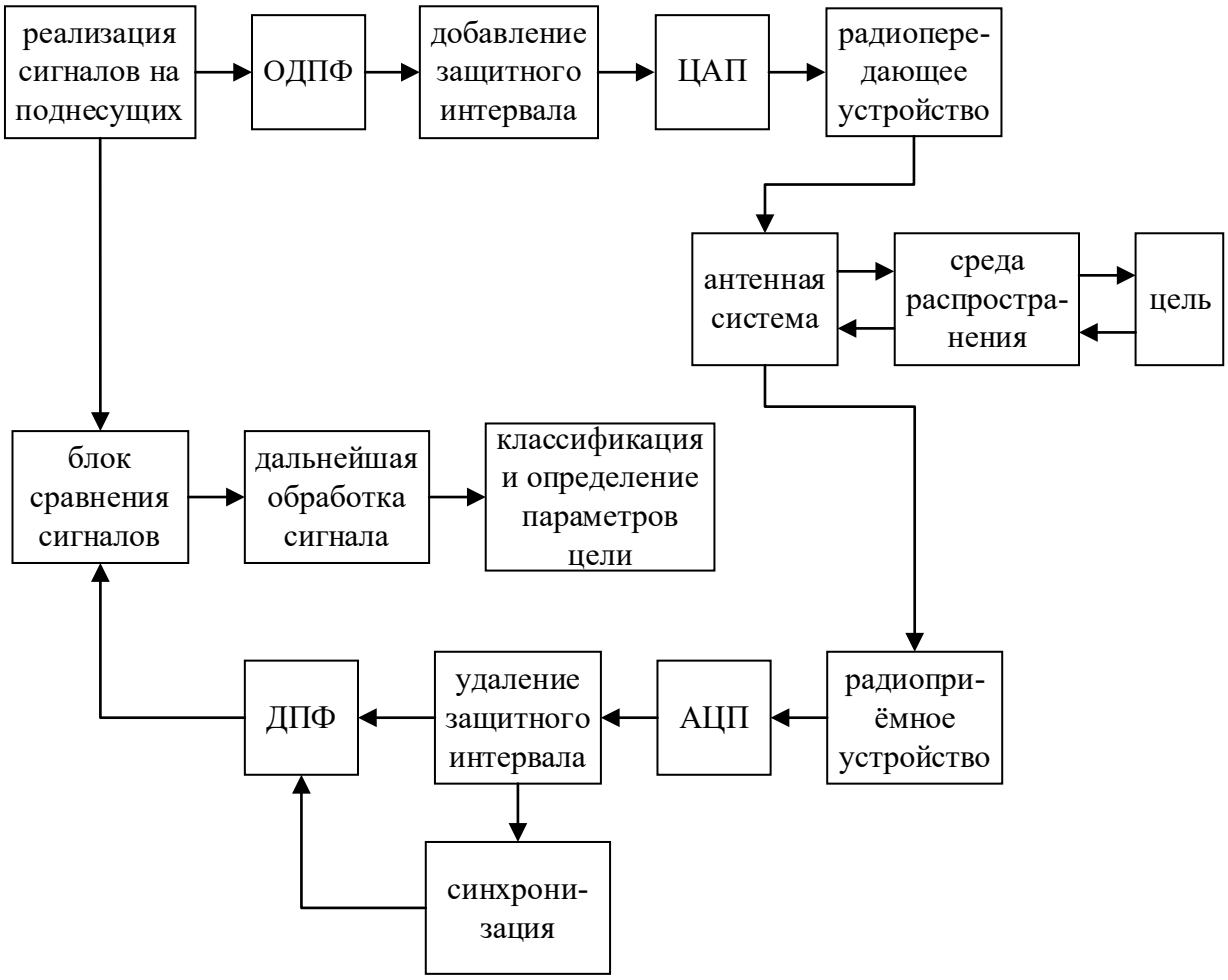

Рисунок 3

Затем следует блок ОДПФ, где формируется *OFDM*-сигнал. Преобразование выполняется с поступающими на вход сигналами. Следующим этапом идет блок добавления защитного интервала. Он необходим, чтобы избежать межсимвольной интерференции. Защитный интервал может быть выполнен в качестве циклического повторения полезной части сигнала, длительность которого может достигать времени длительности полезного сигнала. В частности, по нему можно определять момент начала приема выборки (синхронизация) с принятым сигналом и грубую оценку задержки.

Затем *OFDM*-сигнал проходит в блок ЦАП, переводится в аналоговый вид и подается на радиопередающее устройство. В нем сигнал подготавливается для подачи на антенну. Для этого его необходимо перенести с промежуточной на СВЧ-частоту. Затем сигнал проходит фильтрацию в нужной полосе спектра, чтобы избавится от паразитных гармоник, образовавшихся с переводом центральной

частоты сигнала. После этого сигнал усиливается до необходимой мощности и через согласующее устройство подается на антенную систему.

С антенной системы сигнал излучается в пространство. Там происходит отражение сигнала от местных предметов и от цели, если она присутствует. Распространение в среде сказывается на сигнале: примешиванием шумов, задержкой и доплеровским сдвигом частоты, если объект, от которого отразился сигнал, был в движении. После этого отраженный сигнал поступает обратно на антенную систему. Приема происходит зеркально, относительно передаче.

В радиоприемном устройстве сигнал фильтруется, усиливается и переносится на промежуточную частоту обработки. Затем производится АЦП и аналоговый сигнал переходит в цифровой вид. Далее происходит удаление защитного интервала. Эта отделенная часть принятого сигнала направляется в блок синхронизации, с ее помощью определяется момент времени, чтобы начать операцию ДПФ.

Далее полезная часть сигнала и результат синхронизации поступают на блок ДПФ. В нем *OFDM*-сигнал расформировывается на отдельные поднесущие составляющие, и они подаются на блок, где происходит сравнение исходного и принятого сигналов. Затем сигналы и результаты сравнения поступают на дополнительную обработку в целях классификации объекта, дополнительного анализа и повышения точности оценки параметров цели.

В качестве устройств, на которых можно реализовать описанную обработку сигнала, можно будет использовать высокопроизводительные программируемые логические интегральные схемы (ПЛИС). В частности, могут подойти ПЛИС *Xilinx* серии *Virtex*-5 или более новые, или ПЛИС отечественной разработки серии 5578*ТС* от «КТЦ «ЭЛЕКТРОНИКА». Они уступают по производительности, но можно организовывать параллельные вычисления на нескольких вычислительных системах [19, 20]. Для аналоговой части тоже есть решения по работе с *OFDM*-сигналами, так как они используются почти во всех современных стандартах беспроводной связи. Поэтому не будет проблем подобрать материальную базу для реализации РЛС с не стандартным зондирующим сигналом.

Оценка характеристик разработанной РЛС

В качестве оценок характеристик обнаружения рассматриваемой РЛС можно использовать основное уравнение радиолокации [9]. Часть используемых там параметров были оговорены выше.

$$R_{max} = \sqrt[4]{\frac{P_{\text{пер}} * G_{\text{а}}^2 * \sigma * \lambda^2}{(4\pi)^3 * P_{c\,min} * L_n}}$$

где: $P_{\text{пер}} = 200$ Вт; $G_{\text{а}} = 26$ дБ ≈ 400; $\sigma = 0{,}01$ м^2. Длина волны на частоте 10 ГГц $\lambda \approx 0{,}03$ м. Чувствительность приемника РЛ, составляет $P_{c\,min} \approx 10^{-15}$ Вт [16, 17]. Коэффициент ослабления радиосигнала L_n, который включает в себя потери в атмосфере, в СВЧ тракте при рассогласовании элементов, при детектировании сигнала. Таким образом, общий коэффициент потерь ≈ 10 дБ [9]. В результате расчета получается, что расчетная дальность обнаружения цели с ЭПР 0,01 м^2 при установленных параметрах составляет приблизительно:

$$R_{max} = \sqrt[4]{\frac{200 * 400^2 * 0{,}01 * 0{,}03^2}{(4\pi)^3 * 10^{-15} * 10}} \approx 1{,}95 \text{ км}$$

Если РЛС работает с такими параметрами, то она обеспечивает обнаружение малоразмерного БПЛА на расстоянии 1,95 км и дает время для принятия решения. Например, БПЛА типа «*Switchblade*» способен лететь с максимальной скоростью 160 км/ч. В таком случае дистанцию R_{max} он преодолеет за 44 с. В реальных условиях дальность обнаружения, а значит и время на принятие решения будет, конечно, меньше.

Имеет смысл аналитически рассчитать, дать теоретическую оценку параметрам РЛС, которые она может обеспечить, если применять не типового зондирующий сигнал. Для самой общей оценки можно использовать расчет двумерной автокорреляционной функции (АКФ) – она же функция неопределенности (ФН). Разрешение по дальности и скорости (задержки и частотному сдвигу) можно оценить по области высокой корреляции (уровень 0,5 от максимума), рассчитанной ФН. Стоит учесть, что форма сигнала *OFDM* во временной области зависит от количества поднесущих и комплексных символов модуляции, которые задают фазу на поднесущих колебаниях. Для первичного расчета зададимся случайными символами, но их можно подбирать для определенной формы сигнала. Аналитическая формула для расчета ФН:

$$\psi(\tau, F) = \left| \int_{-\infty}^{\infty} \dot{U}_{OFDM}(t) \dot{U}^{*}_{OFDM}(t-\tau) e^{i2\pi F t}\, dt \right|$$

где: знак * – означает комплексное сопряжение, τ – задержку, а F – частотный сдвиг.

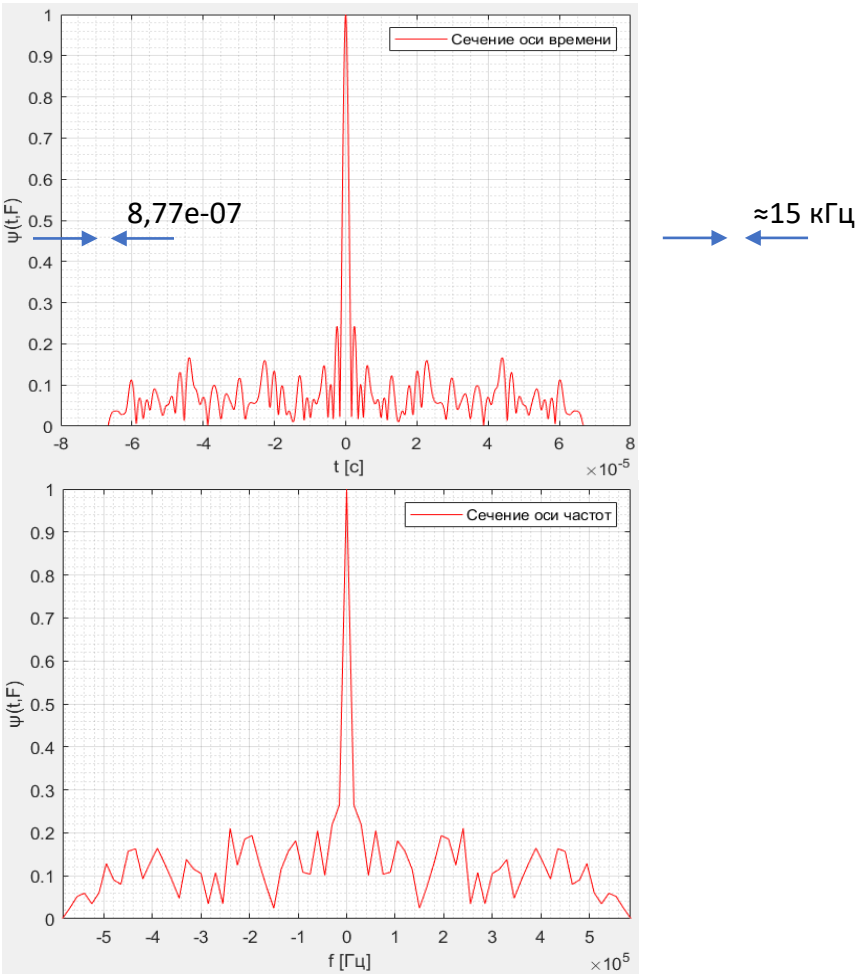

Рисунок 4

У ШП сигналов и сложных кодово-фазомодулированных сигналов, ФН приобретает вид «кнопочной функции», с острым пиком области высокой корреляции [9]. В свою очередь, *OFDM*-сигнал должен иметь такой же вид ФН во временной области. Это означает, что он имеет высокую разрешающую способность.

Чтобы проверить предположение был сформирован *OFDM*-сигнал стандарта *LTE* и построена его ФН при разных параметрах с целью определить изменение характеристики ФН. Параметры сигнала: расстояние между поднесущими 15 кГц; длительность *OFDM*-символа 67 мк с; ширина спектра 1,14 МГц и 2,265 МГц; количество поднесущих, соответственно, 76 и 151. На рис. 4 показаны сечения ФН для сигнала с шириной спектра 1,14 МГц. На рис. 5 показаны сечения ФН для сигнала с шириной спектра 2, 265 МГц.

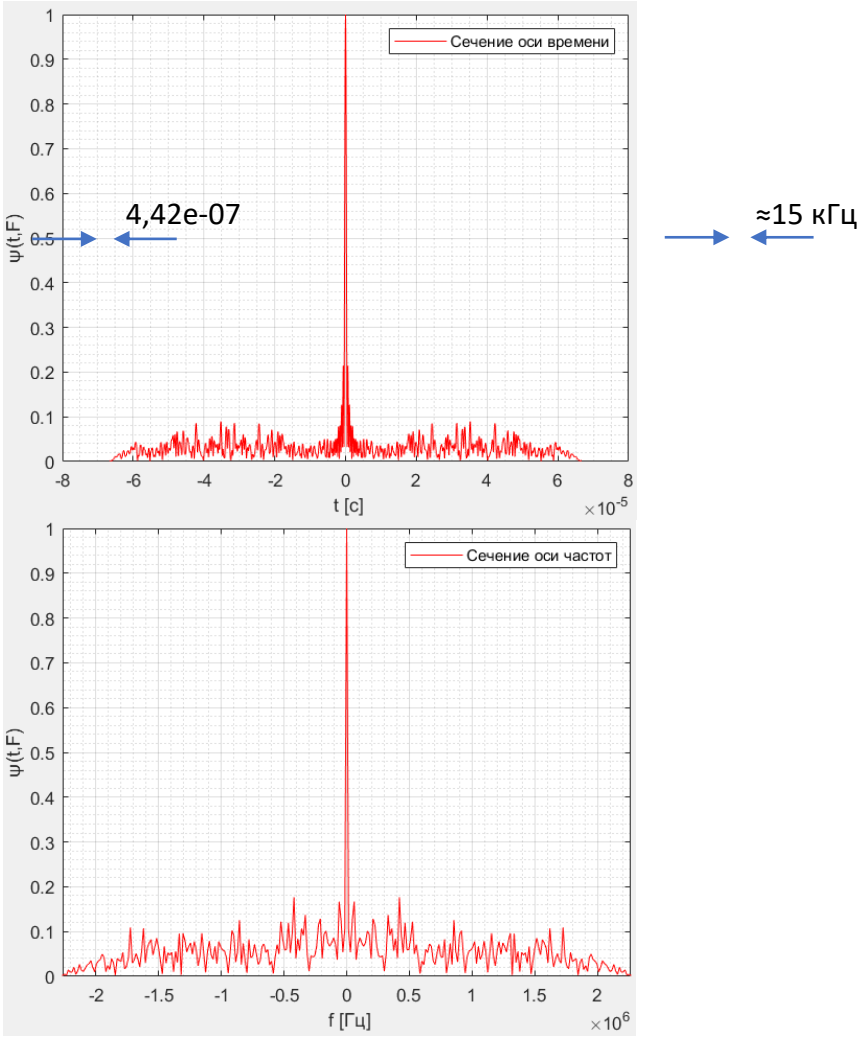

Рисунок 5

Как видно из рис. 4 и 5, с изменением количества поднесущих сигнала ФН меняет вид. С меньшим количеством поднесущих АКФ по задержке приобретает «ножевидную» форме. А с увеличением количества поднесущих она стремится к «кнопочной» и уменьшаются боковые лепестки. В свою очередь, АКФ по частотному сдвигу почти не меняется и имеет «ножевидную» форму. Это происходит из-за формы спектра, близкой к прямоугольной. Ширина области высокой корреляции почти ровна шагу между поднесущими.

Полученные результаты по вычислению сечений ФН дают представление о разрешающей способности сигналов по параметрам цели (табл. 1).

Таблица 1.

Ширина спектра сигнала	**Разрешение по дальности**	**Разрешение по радиальной скорости**
1,14 МГц	131,5 м	225 м/с
2, 265 МГц	65,7 м	225 м/с

Анализируя полученные данные, можно сделать вывод, что, используя сигнал с большим количеством поднесущих, можно добиться разрешающей способности по расстоянию в единицы метров. Но при этом, имеется плохая разрешающая способность по скорости. Прямое корреляционное сравнение спектров принятого и исходного сигналов не смогут различить объекты, двигающиеся с низкой скоростью. Для оценки смещения частоты сигнала требуется применять иные методы.

Сигнал *OFDM* обладает хорошим разрешением по расстоянию. Но с увеличением числа поднесущих, ширина спектра становится больше, мощность сигнала размывается по спектру, и поэтому, нужно искать компромисс между мощностью сигнала и разрешающей способностью.

Заключение

В работе была описана РЛС, которая использует зондирующий ШП *OFDM*-сигнал. Проведен анализ современных целей, которые должна обнаруживать рассматриваемая РЛС. В частности, наиболее актуально проблема обнаружения и отслеживания малоразмерных БПЛА с малой ЭПР. Приведено несколько вариантов исполнения станции и ориентировочно определены ее параметры. Определили максимальную дальность обнаружения малоразмерного БПЛА с ЭПР=0,01м^2, она составила, приблизительно 1,95 км. Обнаружение БПЛА на такой дальности дает время на реакцию, если возникнет экстраординарная ситуация. В частности, был рассмотрен пример с БПЛА типа «*Switchblade*» и определено то, что в теории средствами РЛС его можно будет обнаружить примерно за минуту до подлета к контролируемой территории. Проведена оценка по разрешению параметров сигнала при разных параметрах *OFDM*-сигнала. Форма ФН по задержке стремится к «кнопочной», что говорит о высокой потенциальной возможности определения параметров цели, но по частоте почти не меняется и остается «ножевидной». Дальнейшие исследования будут нацелены на улучшение разрешения по скорости, основанных на косвенных методах оценки смещения частоты.

Литература

1. Бакулин М.Г., Крейнделин В.Б., Шлома А.М., Шумов А.П. Технология OFDM. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2017. – 352 с.
2. Макаренко С.И. Противодействие беспилотным летательным аппаратам. Монография. – СПб: Наукоемкие технологии, 2020. – 204 с.
3. Митрофанов Д.Г., Шишков С.В. Инновационный подход к вопросу обнаружения малогабаритных беспилотных летательных аппаратов // Известия ЮФУ. Технические науки, 2018. – № 1. – С. 28-40.
4. Классификация БПЛА по летным характеристикам // Geoscan URL: https://docs.geoscan.aero/ru/master/database/const-module/classification/classification.html (дата обращения: 03.04.2023).

5. Парнес М. Расчет эффективной поверхности рассеяния малых объектов // СВЧ электроника, 2017. – № 2. – С. 22-24.
6. Методы обнаружения малоразмерных беспилотных летательных аппаратов на основе анализа электромагнитного спектра // Российские беспилотники URL: https://russiandrone.ru/publications/metody-obnaruzheniya-malorazmernykh-bespilotnykh-letatelnykh-apparatov-na-osnove-analiza-elektromagn/
7. Switchblade 300 block 20 loitering munition // URL: https://www.avinc.com/lms/switchblade (дата обращения: 03.04.2023).
8. Сапронов Д.И. Совместное оценивание дальности и скорости в радиолокационных системах с использованием сверхширокополосных дискретно-кодированных по частоте сигналов: дис. канд. техн. наук: 05.12.14. – «Радиолокация и радионавигация». – Москва, 2020. – 112 с.
9. Сперанский В.С. Радиолокация, радиолокационные системы и устройства. – М.: Брис-М, 2011. – 257 с.
10. Подстригаев А.С., Слободян М.Г., Смоляков А.В., Сидорцов И.А. Анализ плотности распределения РЛС военного и специального назначения в частотном диапазоне // Молодой ученый, 2016. – № 27 (131). – С. 136-138.
11. Диапазоны частот и длин волн // radartutorial URL: https://www.radartutorial.eu/07.waves/wa04.ru.html (дата обращения: 9.04.2023).
12. Свойства преобразования Фурье // dsplib.org URL: https://ru.dsplib.org/content/fourier_transform_prop/fourier_transform_prop.html (дата обращения: 09.04.2023).
13. Радиолокационная система «Смерч» на страже ваших объектов // НОЗ.С URL: https://dfnc.ru/popular1/radiolokatsionnaya-sistema-smerch-na-strazhe-vashih-obektov/ (дата обращения: 12.05.2023).
14. «Verba» and «Barnaul-T»: protection of troops in the near zone // top war URL: https://en.topwar.ru/160806-verba-i-barnaul-t-zaschita-vojsk-v-blizhnej-zone.html (дата обращения: 12.05.2023).
15. Багринцев Д. Яковлев К. Особенности энергетического расчета требуемого коэффициента усиления фар СВЧ-диапазона при организации связи с большими подвижными объектами // СВЧ-электроника, 2020. – № 1 (12). – С. 44-45.
16. Ботов М.И. и др. Основы теории радиолокационных систем и комплексов: учеб. Под общ. ред. М.И. Ботова. – Красноярск: Сиб. федер. ун-т, 2013. – 530 с.
17. Тяпкин В.Н. и др. Основы построения радиолокационных станций радиотехнических войск: учебник. Под общ. ред. В.Н. Тяпкина. – Красноярск: Сиб. федер. ун-т, 2011. – 536 с.
18. Кхыонг Н. В. Оценка влияния метеобразования на распространение радиоволн в *X*-диапазоне // Труды МФТИ, 2020. – № 3. – Т. 12. – С. 94-103.
19. Зотов А. Особенности архитектуры нового поколения высокопроизводительных ПЛИС FPGA фирмы Xilinx серии Virtex-6 // Компоненты и технологии, 2009. – № 8. – С. 78-85.
20. Городков П. Особенности разработки HDL-проектов для реализации в базисе ПЛИС серии 5578ТС // Наука | технология | бизнес, 2017. – № 5. – С. 50-59.

РАЗРАБОТКА НЕЙРОСЕТЕВОЙ МОДЕЛИ ДЛЯ ОЦЕНКИ «ИНДЕКСА ЗДОРОВЬЯ» ТРАНСФОРМАТОРНОГО ОБОРУДОВАНИЯ

К.Н. Канатьев, *Нижегородский государственный университет им. Н.И. Лобачевского, basket-player@yandex.ru;*
С.Р. Шишкин, *Московский технический университет связи и информатики, sergeyshishkin62@gmail.com;*
И.С. Дорофеев, *Московский государственный технический университет им. Н.Э. Баумана, ildorof@yandex.ru.*

УДК 621.314

Аннотация. В данной работе представлена разработка нейросетевой модели, направленной на оценку «индекса здоровья» трансформаторного оборудования в энергетических системах. Традиционные подходы к диагностике и мониторингу трансформаторов часто не позволяют своевременно выявлять начинающиеся неисправности, что может привести к серьезным последствиям. В ответ на эти вызовы, в работе исследуются возможности применения современных методов искусственного интеллекта и машинного обучения, включая обучение с учителем, обучение без учителя и обучение с подкреплением, для создания комплексной системы оценки состояния оборудования. Разработанная модель предназначена для анализа данных с датчиков, установленных на трансформаторах, и способна предсказывать потенциальные неисправности, оптимизировать процессы технического обслуживания и повысить надежность энергосистем.

Ключевые слова: трансформаторное оборудование; искусственный интеллект машинное обучение; нейросетевая модель; оценка состояния; диагностика неисправностей; мониторинг оборудования.

DEVELOPMENT OF A NEURAL MODEL FOR ASSESSING THE HEALTH INDEX OF TRANSFORMER EQUIPMENT

Konstantin Kanatev, *Lobachevsky Nizhny Novgorod State University;*
Sergey Shishkin, *Moscow Technical University of Communications and Informatics;*
Ilia Dorofeev, *Bauman Moscow State Technical University.*

Annotation. This paper presents the development of a neural network model aimed at assessing the health index of transformer equipment in power systems. Traditional approaches to diagnostics and monitoring of transformers often fail to timely detect emerging faults, which can lead to serious consequences. In response to these challenges, this work explores the possibilities of applying modern artificial intelligence and machine learning methods, including supervised learning, unsupervised learning, and reinforcement learning, to create a comprehensive system for assessing the condition of the equipment. The developed model is designed to analyze data from sensors installed on transformers and is capable of predicting potential faults, optimizing maintenance processes, and increasing the reliability of power systems.

Keywords: transformer equipment; artificial intelligence; machine learning; neural network model; condition assessment; fault diagnosis; equipment monitoring.

Введение

Трансформаторное оборудование играет важнейшую роль в распределительных сетях, обеспечивая необходимое преобразование

электроэнергии для ее эффективной передачи и потребления. Однако, из-за своей критической роли и высоких требований к бесперебойной работе, трансформаторы становятся уязвимыми звеньями системы, где любой сбой может привести к серьезным последствиям, включая экономические потери и риски для безопасности.

Традиционные методы диагностики и мониторинга трансформаторов основаны на регулярных физических осмотрах и анализе рабочих параметров, таких как температура, уровень изоляционного масла и электрические характеристики. Хотя эти методы оказались эффективными в определенных аспектах, они не всегда могут своевременно выявить начинающиеся неисправности или предсказать вероятность будущих отказов.

В последние годы значительные достижения в области искусственного интеллекта и машинного обучения открыли новые возможности для совершенствования систем мониторинга и диагностики. Использование нейронных сетей для анализа данных с датчиков позволяет не только обнаруживать сложные шаблоны и аномалии, которые могут указывать на потенциальные неисправности, но и предсказывать будущие события на основе обработки больших объемов исторических данных.

Целью данного исследования является разработка инновационной нейросетевой модели, способной анализировать разнообразные данные о состоянии трансформаторного оборудования для оценки его «индекса здоровья». Этот подход предполагает создание комплексной системы, которая будет способствовать не только предотвращению возможных неисправностей и снижению риска аварийных ситуаций, но и оптимизации процессов технического обслуживания, повышению эффективности использования оборудования и, в конечном итоге, улучшению качества и надежности электроснабжения.

Выбор архитектуры модели

Для достижения поставленных целей было решено рассмотреть несколько типов нейронных сетей, каждая из которых обладает своими преимуществами в обработке временных рядов и многомерных данных. В итоге, внимание было сосредоточено на следующих архитектурах:

- Сверточные нейронные сети (*CNN*)

Благодаря своей способности выявлять иерархические шаблоны в данных, эти сети идеально подходят для анализа изображений и могут быть применены для обработки временных рядов, представленных в виде «изображений» активности параметров оборудования.

- Рекуррентные нейронные сети (*RNN*) и сети с долгой кратковременной памятью (*LSTM)*

Эти архитектуры показывают высокую эффективность в анализе временных рядов благодаря своей способности сохранять информацию из предыдущих шагов, что критически важно для отслеживания динамики изменений в работе трансформаторов.

В табл. 1 приведен анализ нейронных сетей.

Таблица 1.

Тип нейронной сети	**Преимущества**	**Подходит для**
Сверточные нейронные сети (*CNN*)	Идеально подходят для анализа изображений и могут быть применены для обработки временных	Анализа изображений, обработки временных

Тип нейронной сети	Преимущества	Подходит для
	рядов, представленных в виде «изображений» активности параметров оборудования.	рядов в формате изображений.
Рекуррентные нейронные сети (*RNN*)	Эффективны в анализе временных рядов, могут обрабатывать данные с временными зависимостями, благодаря способности возвращать информацию на предыдущие шаги.	Анализа временных рядов с короткими временными зависимостями.
Сети с долгой кратковременной памятью (*LSTM*)	Подобно *RNN*, но с улучшенной способностью к сохранению информации на длительные периоды без затухания, что критически важно для отслеживания динамических процессов.	Анализа временных рядов с длительными временными зависимостями и комплексной динамикой.

Данная таблица подчеркивает уникальные характеристики каждой архитектуры нейронной сети и их пригодность для определенных видов анализа данных. В контексте мониторинга и диагностики трансформаторного оборудования, выбор между этими архитектурами будет зависеть от специфики задачи, доступности данных и желаемой точности предсказаний.

Методы обучения

В разработке модели были применены следующие подходы к обучению:

- Обучение с учителем. Данная методика была выбрана для первоначального обучения модели на основе исторических данных, содержащих аннотации о состоянии оборудования. Это позволило эффективно настроить параметры модели для распознавания специфических шаблонов, ассоциируемых с различными состояниями трансформаторов.
- Обучение без учителя. Для дальнейшего уточнения модели и выявления неизвестных или ранее не встречавшихся шаблонов поведения оборудования применялся подход без учителя. Это позволило обнаружить скрытые корреляции и аномалии в данных, которые могут указывать на начинающиеся неисправности.
- Обучение с подкреплением. В качестве экспериментальной методики рассматривалось обучение с подкреплением для оптимизации процесса принятия решений моделью в реальном времени. Этот подход предполагает корректировку поведения модели на основе обратной связи от энергетической системы, что позволяет постоянно совершенствовать качество предсказаний.

Сбор и подготовка данных для нейросетевой модели

В основе успешного создания и функционирования нейросетевой модели для оценки «индекса здоровья» трансформаторного оборудования лежит качественно подготовленный и всесторонний набор данных. Важность этого этапа обусловлена необходимостью обучения модели распознаванию широкого спектра условий работы оборудования, включая нормальные рабочие параметры и признаки потенциальных неисправностей.

Данные для обучения и тестирования модели могут быть собраны из различных источников:

- *Исторические данные.* Архивные записи о работе трансформаторного оборудования, включая отчеты о неисправностях, данные о регулярных технических осмотрах, анализы изоляционного масла и результаты электрических измерений.
- *Данные с датчиков.* Современное трансформаторное оборудование обычно оснащено множеством датчиков, собирающих реальные данные во время эксплуатации. Это могут быть показатели температуры, давления, уровня изоляционного масла, параметры электрической нагрузки и многие другие.

Подготовка данных включает несколько ключевых этапов, каждый из которых играет важную роль в создании эффективной модели:

- *Очистка данных.* На этом этапе данные очищаются от аномалий, ошибок измерений и прочих артефактов, которые могут исказить результаты обучения. Это включает удаление или коррекцию выбросов, а также обработку пропущенных значений.
- *Нормализация.* Данные из различных источников и с разных датчиков могут иметь различный масштаб, что может негативно сказаться на процессе обучения. Нормализация данных помогает привести все показатели к единому масштабу, облегчая тем самым задачу для нейросети.
- *Преобразование данных.* В зависимости от выбранной архитектуры нейросети, может потребоваться преобразование собранных данных в определенный формат. Например, для *CNN* временные ряды могут быть преобразованы в «изображения» активности параметров, в то время как для *RNN* или *LSTM* данные представляются в виде последовательностей.
- *Разделение данных.* Наконец, готовый датасет разделяется на обучающую, валидационную и тестовую выборки. Это позволяет не только обучить модель, но и оценить ее способность к обобщению на новых данных.

Предварительная обработка данных в контексте разработки нейросетевой модели

Предварительная обработка данных является неотъемлемой частью процесса подготовки к обучению нейросетевой модели. Этот этап направлен на улучшение качества данных путем их очистки, нормализации и преобразования, что в свою очередь способствует повышению точности и эффективности обучения. Рассмотрим подробнее каждый из аспектов предварительной обработки данных.

Очистка данных от шума и аномалий является первым шагом в процессе предварительной обработки. Шум может появляться в результате ошибок измерения, неисправностей датчиков или внешних помех. Для идентификации и удаления шума применяются различные методы, включая статистический анализ, фильтрацию и использование алгоритмов машинного обучения, способных распознавать и исключать аномальные значения из набора данных.

Пропущенные значения в данных могут возникать по различным причинам, включая сбои в работе датчиков и ошибки при сборе или передаче данных. Существует несколько подходов к заполнению пропусков, среди которых:

- Использование средних значений или медиан по соответствующим параметрам.
- Применение методов интерполяции для восстановления отсутствующих значений на основе соседних по времени записей.
- Использование алгоритмов машинного обучения для предсказания пропущенных значений, учитывая зависимости между различными параметрами.

Нормализация данных предполагает приведение всех измерений к единому масштабу, что необходимо для корректной работы большинства алгоритмов машинного обучения. Это достигается путем преобразования значений каждого признака таким образом, чтобы их распределение имело заданное среднее значение и стандартное отклонение, либо путем масштабирования в заданный диапазон. Нормализация улучшает сходимость алгоритмов обучения и повышает общую точность модели.

Завершающим этапом предварительной обработки является преобразование данных в формат, наиболее подходящий для выбранной архитектуры нейросети:

- Для *CNN* временные ряды могут быть преобразованы в «изображения» активности параметров оборудования, позволяя модели эффективно выявлять сложные шаблоны и зависимости.
- Для рекуррентных нейронных сетей (*RNN*) и сетей с долгой кратковременной памятью (*LSTM*) данные подготавливаются в виде последовательностей, что позволяет учитывать временные зависимости между различными наблюдениями.

Обучение нейросетевой модели для диагностики трансформаторного оборудования

В разработке нейросетевой модели для оценки состояния трансформаторного оборудования ключевым этапом является обучение, в ходе которого модель «изучает» закономерности в данных, позволяющие ей делать точные предсказания и выявлять потенциальные неисправности. В зависимости от специфики задачи и характера доступных данных, могут быть применены различные подходы к обучению: обучение с учителем, обучение без учителя и обучение с подкреплением. Каждый из этих методов имеет свои особенности и области применения.

Обучение с учителем предполагает наличие размеченного набора данных, где каждому входному образцу соответствует определенный «правильный» ответ (например, указание на нормальное состояние оборудования или на конкретный вид неисправности). В процессе обучения модель стремится минимизировать различие (ошибку) между своими предсказаниями и реальными данными, постепенно улучшая свою способность к распознаванию различных состояний оборудования. Этот подход особенно эффективен при наличии обширного и хорошо размеченного датасета, позволяя модели достигать высокой точности в задачах классификации и регрессии.

В отличие от обучения с учителем, обучение без учителя не требует наличия размеченных данных. Вместо этого модель анализирует входные данные, пытаясь самостоятельно выявить в них закономерности, группы похожих объектов или аномалии. Этот метод часто используется для задач кластеризации, снижения размерности данных и обнаружения аномалий. В контексте мониторинга трансформаторного оборудования обучение без учителя может помочь выявить нестандартные модели поведения оборудования, которые могут указывать на начинающиеся неисправности.

Обучение с подкреплением отличается от предыдущих подходов тем, что модель обучается на основе взаимодействия с окружающей средой, стремясь максимизировать некоторый кумулятивный выигрыш или «награду». В контексте диагностики оборудования этот метод может быть использован для оптимизации процессов принятия решений, например, для определения оптимального графика технического обслуживания на основе текущего состояния оборудования и его

эксплуатационной истории. Обучение с подкреплением позволяет модели адаптироваться к изменениям в работе оборудования, постепенно улучшая стратегию принятия решений.

Заключение

Разработка нейросетевой модели для оценки «индекса здоровья» трансформаторного оборудования демонстрирует значительный потенциал применения методов искусственного интеллекта и машинного обучения в энергетической отрасли. Применение такой модели позволяет не только повысить эффективность и надежность диагностики состояния оборудования, но и способствует оптимизации процессов технического обслуживания, снижению риска возникновения аварийных ситуаций и улучшению общей безопасности и устойчивости энергосистем. Результаты исследования показывают, что интеграция современных технологий в процессы мониторинга и управления состоянием трансформаторного оборудования открывает новые горизонты для повышения эффективности и надежности энергетической инфраструктуры.

Литература

1. Красноярская ГЭС // Википедия URL: ru.wikipedia.org/wiki/Красноярская_ГЭС (дата обращения: 15.01.2023).
2. История строительства Красноярской ГЭС // 6000megawatt.kkkm.ru URL: 6000megawatt.kkkm.ru/ (дата обращения: 15.01.2023).
3. Красноярская ГЭС // Ассоциация «Гидроэнергетика России» URL: www.hydropower.ru/stations/detail.php?ELEMENT_ID=1921 (дата обращения: 15.01.2023).
4. Бостром Ник. Искусственный интеллект. Этапы. Угрозы. Стратегии. – Москва: Мир, 2021. – 119 с.

ИНФОРМАЦИОННЫЕ СИСТЕМЫ, СЕТИ И ТЕХНОЛОГИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ

ИССЛЕДОВАНИЕ ПРИМЕНЯЕМЫХ ГОСУДАРСТВАМИ МЕТОДОВ И ТЕХНИЧЕСКИХ ОСОБЕННОСТЕЙ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Н.В. Евглевская, *к.т.н., Военная академия связи им. Маршала Советского Союза С.М. Буденного, n.evglevskaya@gmail.com;*
Д.А. Остроухов, *Национальный исследовательский университет ИТМО, demid-ostrouhov@yandex.ru;*
С.Н. Ракицкий, *к.в.н., доцент, Военная академия связи им. Маршала Советского Союза С.М. Буденного, s15136@mail.ru.*

УДК 004.056.57

Аннотация. Все большее число правительств по всему миру прибегают к хакерским атакам для облегчения своей правоохранительной и другой деятельности, связанной с безопасностью граждан и государства. В статье рассматриваются методы правительственного взлома. Особое внимание уделено наиболее распространенным в различных странах программным средствам, применяемым при правительственном взломе, их техническим особенностям.

Ключевые слова: правительственный взлом; вредоносное программное обеспечение; бэкдор; эксплойт; оперативно-разыскная деятельность.

RESEARCH OF METHODS AND TECHNICAL FEATURES OF CRIMINAL INTELLIGENCE OPERATIONS USED BY STATES

Natalya Evglevskaya, *candidate of Engineering, The Military Academy of Telecommunications named after Marshal of the Soviet Union S.M. Budyonny;*
Demid Ostroukhov, *ITMO National Research University;*
Stanislav Rakitsky, *candidate of military sciences, associate Professor, The Military Academy of Telecommunications named after Marshal of the Soviet Union S.M. Budyonny.*

Annotation. An increasing number of governments around the world are resorting to hacker attacks to facilitate their law activity related to the security of citizens and state. The article discusses the methods of government hacking. Special attention is paid to the prevailing software tools used in various countries, their technical features.

Keywords: government hacking; malware; backdoor; exploit; intelligence-gathering activities.

Введение

В настоящее время правительство многих стран прибегают к хакерским атакам, что связано с безопасностью граждан и государства. Но многие используют этот потенциал тайно и без четких правовых оснований. В тех случаях, когда правительства стремятся закрепить такие полномочия на законодательной основе, они часто делают это без гарантий и надзора, применимых к подобного рода

действиям в соответствии с международным законодательством в области прав человека.

Взлом может представлять собой уникальную и серьезную угрозу конфиденциальности и безопасности данных. Поэтому, даже в тех случаях, когда правительства применяют вышеупомянутые подходы в связи с законной деятельностью, такой как сбор доказательств в рамках уголовного расследования или разведывательных данных, они вряд ли смогут продемонстрировать, что хакерство, как форма деятельности по обеспечению безопасности, совместимо с международным законодательством в области прав человека. Однако на сегодняшний день не было проведено публичных дебатов о масштабах и характере таких полномочий и их последствий для конфиденциальности и безопасности данных граждан, государства и международного сообщества в целом.

Когда дело доходит до описания методов и тактик, используемых государствами и их правоохранительными органами для правительственного взлома, можно столкнуться с двумя трудностями. Одна из них заключается в том, что методы, которые используют государственные органы, являются государственной тайной и, как следствие, засекречены. Во-вторых, каждое государство имеет разные мотивы, когда дело доходит до инициирования правительственного взлома, и, следовательно, использует разные тактики [1].

Накопление или эксплуатация уязвимостей

В 2017 г. интернет захлестнула настоящая эпидемия файлов с расширением *Wcry* (закодированные файлы). Отсюда и пошло название шифровальщика – *WannaCry*. Атака затронула больницы, предприятия, университеты и многие другие общественно значимые сферы общества. Инцидент с *WannaCry* вызывает особый интерес, так как вредоносное воздействие было украдено у Агентства национальной безопасности (АНБ) Соединенных Штатов Америки. В связи с данным событием актуализировался вопрос: должны ли государства накапливать знания об уязвимостях программного обеспечения (ПО) и программном обеспечении для их использования?

Аргумент в пользу наличия у государств этих запасов такой же, как аргумент, используемый для оправдания накопления традиционного вида оружия, оружия массового поражения. Общая идея заключается в том, что такие запасы необходимы для национальной безопасности: для защиты и продвижения интересов государства. В случае использования уязвимостей для шпионажа, аргумент безопасности можно изменить, проведя аналогию с другими методами шпионажа. Как должно быть очевидно, в той мере, в какой государства имеют право накапливать физическое оружие и заниматься шпионажем в целях своей безопасности, они, по-видимому, также имеют право накапливать программное оружие и знания об уязвимостях.

Очевидный моральный контраргумент может быть построен на следующих основаниях: вред, причиняемый при краже и распространении такого ПО и информации, превышает выгоды, получаемые государствами, имеющими это ПО и информацию. Инцидент с *WannaCry* служит прекрасным примером. В то время, когда АНБ имело кратковременное преимущество, обладая исключительным правом собственности на ПО и информацию, ущерб, нанесенный вымогателями миру, безусловно, превышает это небольшое временное преимущество. Учитывая масштаб ущерба, который может быть нанесен, вред, причиняемый украденным ПО и информацией, как правило, превышает выгоды для государств. Таким образом, накопление такого ПО и знание уязвимостей является морально неправильным.

Однако, государствам просто необходимо обезопасить свое ПО и информацию, используемую в качестве оружия. Точно так же, как государство обязано гарантировать, что его традиционное вооружение не может быть использовано в преступных или террористических целях, государство обязано гарантировать, что его ПО и информация об уязвимостях не будут украдены. Таким образом, государствам приемлемо иметь кибероружие, как и обычное оружие.

Компьютерная сеть, формирующая нервную систему современного мира, слишком важна для всех, чтобы подвергать ее риску ради относительно незначительных и краткосрочных выгод, которые могли бы получить государства, создающие вредоносные программы и накапливающие уязвимости [2].

Социальные риски, связанные с уязвимостями в информационных системах и применяемыми средствами защиты, можно увидеть, проведя параллель с балансом рисков с биологическим оружием и государственными программами по укреплению и охране здоровья населения.

В микробиологии в случае обнаружения патогенного микроорганизма, опасных инфекций, требуется время для разработки вакцины. А после разработки вакцины требуется время для проведения вакцинации населения. То же самое применительно и по отношению к уязвимостям ПО: требуется время для разработки исправлений, а также время для развертывания исправления после его разработки. Программа вакцинации никогда не может быть универсальной точно так же, как данный патч никогда не может быть установлен на каждом уязвимом сетевом компьютере на планете.

Также возможно взять патогенный микроорганизм и «превратить» его в оружие, например, расширив диапазон температур, при которых он остается жизнеспособным, или просто создав «бомбы» для доставки, способные быстро распространить его по определенной территории. А уже вакцинированное население не уязвимо к биологическому оружию.

Предполагается, что наши правительственные учреждения должны защищать нас. Они знают, что эти уязвимости опасны. Хотим ли мы, чтобы они отложили создание программ вакцинации только для того, чтобы иметь запас эффективного оружия для использования в будущем?

Что, если бы Минздрав России в дополнение к своей текущей деятельности по сохранению здоровья и долголетия граждан, отвечал за разработку и накопление биологического оружия для использования против различных категорий граждан? Лучше или хуже, когда одно и то же агентство несет ответственность как за защиту нашего общества, так и за сохранение его уязвимости? Что должно произойти, если какая-либо часть государства или независимый исследователь обнаружит особенно опасный микроб – следует ли проинформировать Минздрав? Должен ли государственный орган, обнаруживший такой микроб, рассматривать возможность сохранения его в секрете, чтобы оно могло использовать его против людей, которых оно считает «плохими», хотя остальная часть населения также уязвима? Какой стимул у независимого исследователя, заботящегося о безопасности, делиться таким пугающим открытием с Минздравом, если он знает, что министерство может принять решение использовать опасную информацию в негативных целях, а не для защиты здоровья населения?

Что, если бы государство активно создавало биологическое оружие, разрабатывая способы его более широкого распространения или создавая эффективные средства его доставки?

Эти виды оружия не могут быть применены без определенного риска их распространения, вот почему биологическое оружие было запрещено международной конвенцией. Тот, кто подвергся воздействию микроба, может

культивировать его и производить больше. Тот, кто подвергся воздействию вредоносного ПО, может создать копию, проверить ее, модифицировать и повторно развернуть. Должны ли мы мириться с такого рода деятельностью государств, отвечающих за общественную безопасность? К сожалению, этот вопрос на данный момент на международной арене обсуждается недостаточно активно, несмотря на тот факт, что несколько государств накапливают уязвимости и используют их против информационных систем в общедоступной сети [3].

Вредоносное программное обеспечение

В общих чертах, вирусные программы – это вредоносные программы, которые каким-либо образом вредят или делают нечто нежелательное в аппаратном и ПО легальных пользователей. Большинство людей знают о вирусах, троянах, программах, крадущих информацию, и даже программах, которые шифруют данные и требуют деньги за их восстановление. За последние несколько лет стали широко известны вирусы, использующиеся для слежения, или шпионские программы. Это программы, которые устанавливают на компьютер не киберпреступники, а государственные органы безопасности или полиция. Они дают им доступ к коммуникациям пользователя в сети и, поскольку жизнь сейчас в большой степени проходит в интернете, то там государство в основном и занимается слежкой.

Вредоносные шпионские программы могут иметь широкий спектр возможностей. Например, поскольку мобильные телефоны теперь все реже используются для телефонных звонков, а все больше для общения в интернете, наблюдается рост количества шпионских программ для, так называемого, «полицейского перехвата». Если на телефон тайно установлена подобная программа, то она позволяет следить за перемещениями пользователя через *Global Positioning System GPS*, просматривать список контактов, читать *SMS*-сообщения, записывать телефонные разговоры, видеть переписки в социальных сетях и многое др. [4].

Внедрение вредоносного ПО состоит из нескольких этапов: доставка, эксплуатация, исполнение и отчетность.

Первый этап. Доставка. Уполномоченный государственный орган должен сначала доставить свое вредоносное ПО до цели, как правило в сообщении, отправляемом подозреваемому. Сообщение включает описание, предназначенное для того, чтобы принудить жертву перейти по ссылке, которая перенаправляет ее веб-браузер на веб-сайт или контент, контролируемый правоохранительными органами. Этот тип доставки вредоносных программ, получивший название «фишинг» в области компьютерной безопасности, нацелен на конкретных лиц.

Более сложная тактика правоохранительных органов заключается в следующем. Идентифицируется оператор интернет-ресурса, подвергается захвату его инфраструктура, но в тоже время интернет-ресурс продолжает работу с добавленным вредоносным кодом. Когда подозреваемые взаимодействуют с веб-сайтом при определенных условиях запуска – например, посещая его при входе в систему или переходя на определенные веб-страницы – вредоносное ПО доставляется до подозреваемого. Таким образом, в отличие от фишинговой атаки, этот тип атаки нацелен на любых лиц, которые ведут себя определенным образом.

Второй этап. Эксплуатация. В начале реализации данного этапа правоохранительным органами известно следующее. ПО поступает из различных источников, не всем разработчикам можно доверять. Как следствие, ПО обычно выполняется с ограниченными разрешениями: оно может получать доступ только к определенным данным и функциональным возможностям на устройстве. Веб-

браузеры и мобильные устройства устанавливают особенно строгие правила безопасности, требуя, чтобы ПО было написано на определенных языках и предоставляло доступ только к определенным возможностям. Веб-браузеры, например, обычно запускают только ПО, написанное на языке *JavaScript*, и предоставляют этому ПО доступ только к сохраненным данным, связанным с источником ПО. Некоторые функции, такие как включение веб-камеры устройства и *GPS*, доступны только с согласия пользователя. Другие возможности устройства, такие как чтение данных из сторонних приложений, полностью запрещены. Вводя эти ограничения, службы безопасности устройства одновременно соответствуют ожиданиям пользователя в отношении безопасности и конфиденциальности и информируют о них.

Взлом правоохранительными органами обязательно подрывает барьеры безопасности, чтобы предоставить следователям доступ к необходимым им данным и функциям. Разработчики вредоносных программ выявляют или приобретают уязвимости в приложениях, которые позволяют им обходить защиту устройств. Конкретная уязвимость в системе безопасности устройства, которую использует государство, и то, как оно использует эту уязвимость, зависят от множества факторов, включая информацию, которую ищут следователи, и конфигурацию ПО, используемого подозреваемыми.

Третий этап. Исполнение. Как только правоохранительные органы обходят средства защиты, их ПО запускается. Простой экземпляр вредоносного ПО может отметить время запуска ПО, собрать информацию об ОС и процессоре, а затем отправить сетевой запрос, содержащий *IP*-адрес устройства.

Более изощренные вредоносные программы могут извлекать дополнительную идентифицирующую информацию через ОС устройства. Такими данными могут быть: имя компьютера и уникальный идентификатор, который производитель компьютера присвоил его сетевой карте и др.

Четвертый этап. Отчетность. Наконец, когда ПО правоохранительных органов запустилось на устройстве подозреваемого, оно обращается посредством сети интернет к правоохранительным органам, инициировавшим применение данного ПО, чтобы сообщить информацию о расследовании. Для решения этой задачи подходит любой сервер, контролируемый государством.

Перечисленные четыре этапа: доставка, эксплуатация, исполнение и отчетность, являются основополагающими для функционирования правительственного вредоносного ПО. И каждый шаг потенциально может привести к непредвиденным последствиям, включая угрозы безопасности и конфиденциальности данных граждан [5].

Бэкдоры

Современное шифрование не только защищает информацию от злоумышленников, оно также не позволяет правоохранительным органам ознакомиться с данными граждан. Даже, когда правоохранительные органы получают разрешение на данные действия со стороны суда, это не помогает им расшифровывать данные граждан. Такое ограничение находится в центре продолжающихся дебатов о надлежащей роли шифрования в обществе, которые впервые начались в 1990-х гг.

Сторонники правоохранительных органов утверждают, что шифрование представляет фундаментальную угрозу общественной безопасности, поскольку санкционированные судом расследования не могут быть проведены. Защитники конфиденциальности и представители бизнеса подчеркивают важность шифрования для обеспечения личной неприкосновенности, защиты деловых

операций и ограничения власти правоохранительных органов. В попытке удовлетворить обе потребности, правоохранительные органы настаивали на использовании специальных «бэкдоров» в зашифрованных системах, то есть специального метода дешифрования, который может использоваться правоохранительными органами только при выполнении санкционированных судом оперативно-разыскных действий.

В основе этих социально-политических дебатов лежит технический вопрос: возможно ли создать надежную систему шифрования с «бэкдором», который могут использовать только правоохранительные органы? За последние 30 лет был достигнут незначительный прогресс в ответе на этот вопрос. Большинство предлагаемых конструкций систем шифрования с «бэкдорами» предоставляют государству ключи шифрования, которые могут расшифровать все, в надежде, что никто не воспользуется ключами не по назначению. Подавляющее большинство исследователей и активистов согласны с тем, что этот подход по своей сути ошибочен, так как существует слишком много способов злоупотребления ключами шифрования.

Прогресс в решении этого технического вопроса застопорился, поскольку требования к желаемым системам так и не были полностью определены. Иными словами, на самом деле есть два вопроса, маскирующихся под один: (1) какие свойства должны обеспечивать системы шифрования с «бэкдорами» правоохранительных органов? и (2) возможно ли построить системы, которые обеспечивают эти свойства? Редко можно увидеть четкий и связный ответ на первый вопрос и консенсуса нет. Это затрудняет переход ко второму вопросу.

Однако можно определить минимальные свойства, которыми должны обладать зашифрованные системы:

Доступ правоохранительных органов к конфиденциальным данным граждан возможен только при наличии разрешения суда. Зашифрованный контент по умолчанию должен оставаться полностью защищенным. Правоохранительные органы – и только правоохранительные органы – должны иметь возможность использовать ключи шифрования, если соответствующее разрешение выдано соответствующим судом.

Выявляемость злоупотреблений. Огромная проблема с существующими предложениями заключается в том, что злоупотребления могут происходить скрытно; конкретный работник правоохранительных органов может использовать ключи шифрования в своих целях и никто никогда не узнает об этом.

Системы должны требовать создания общедоступного следа прежде, чем можно будет использовать «бэкдор». Этот след позволит аудиторам поднимать тревогу при обнаружении неправомерного использования.

Глобальная политика выдачи разрешений судами. Как общество, нам необходимо договориться о том, как должны выглядеть эти разрешения. Например, возможно, мы хотим ограничить выдачу разрешений конкретными лицами. Возможно, мы хотим, чтобы разрешения можно было использовать только в течение коротких периодов времени. Определив некоторую глобальную политику выдачи разрешений, мы можем ограничить разрушительные возможности суда или правоохранительных органов.

Криптографическое обеспечение. (Теоретически) легко написать закон, который требует, чтобы система обладала указанными выше свойствами. К сожалению, в первую очередь необходимо позаботиться о предотвращении злоупотреблений системой со стороны лиц, которые не уважают закон. Таким образом, необходимо разработать технические системы, которые обеспечивают соблюдение всех этих свойств, используя что-то более надежное, чем закон,

например математику. Другими словами, необходимо, чтобы математика, используемая для построения системы, делала ключи шифрования непригодными для использования, если судебное разрешение не соответствует политике разрешения или не был создан контрольный журнал.

Развертывание «бэкдора» правоохранительных органов без этих минимальных свойств защиты от злоупотреблений, несомненно, является прямым путем к катастрофе. Прежде чем начать обсуждение того, как внедрять «бэкдоры», крайне важно согласовать минимальные свойства защиты от злоупотреблений для такой системы [6].

***Pegasus* (*NSO Group*, Израиль)**

Pegasus – шпионская программа, которую можно незаметно установить на мобильные телефоны и другие устройства, работающие под управлением некоторых версий мобильных операционных систем (ОС) *iOS* и *Android*. Разработчиком *Pegasus* является израильская компания *NSO Group*. Компания заявляет, что предоставляет «уполномоченным правительствам технологии, которые помогают им бороться с терроризмом и преступностью», она также опубликовала фрагменты условий применения программы, требующих от клиентов использовать *Pegasus* только в целях уголовной и национальной безопасности. *NSO Group* также утверждает, что соблюдает права человека [7].

Атака очень проста в осуществлении. Она начинается, когда злоумышленник отправляет *URL* веб-сайта (через *SMS*, электронную почту, социальные сети или любое другое сообщение) идентифицированной цели. Пользователю нужно выполнить только одно действие – нажать на ссылку. Как только пользователь нажимает на ссылку, ПО незаметно выполняет серию эксплойтов против устройства жертвы для удаленного взлома устройства компании *Apple*, чтобы можно было установить пакеты шпионского ПО. Единственным признаком того, что что-то произошло, будет закрытие браузера после перехода по ссылке.

Для достижения цели программа-шпион после взлома телефона пользователя не загружает вредоносные версии этих приложений на устройство жертвы с целью захвата данных, а компрометирует исходные приложения, уже установленные на устройстве. Сюда входят предустановленные приложения, такие как *Facetime* и *Calendar*, а также приложения из официального *App Store*.

Пользователь, зараженный этим шпионским ПО, находится под полным наблюдением злоумышленника, поскольку в дополнение к перечисленным выше приложениям, он также следит за:

- телефонными звонками;
- журналами вызовов;
- *SMS*-сообщениями, которые отправляет или получает жертва;
- аудио- и видеосвязью, которая (по словам основателя *NSO Group*) превращает телефон в «портативную рацию».

Доступ к указанному контенту может быть использован для получения дальнейшего доступа к другим учетным записям жертвы, принадлежащим цели, таким как банковские услуги, электронная почта и другие сервисы, которыми она может пользоваться на устройстве или вне его [8].

***FinSpy* (*FinFisher*) (*Vilicius Holding GmbH*, Германия)**

FinSpy – коммерческая шпионская программа, которой пользуются силовые структуры и государственные органы разных стран. Впервые она попала на радары

исследователей в 2011 г., когда на *Wikileaks* появились связанные с ней документы. В 2014 г. исходный код зловреда выложили в интернет, однако на этом его история не закончилась: разработчики переписали *FinSpy* и он до сих пор продолжает заражать устройства по всему миру.

FinSpy не ограничивается одним методом заражения. Имеется сразу три пути, которые шпионская программа использует, чтобы проникнуть на компьютеры с ОС *Windows* [9].

Вредоносная программа создает копию исходной главной загрузочной записи и сохраняет ее в другом месте на жестком диске. Кроме того, вредоносная программа записывает 0x2*A*00 байт данных на зараженный жесткий диск. Эти данные позже копируются вредоносным загрузочным кодом. Адрес первого сектора, содержащего эти данные, жестко закодирован в коде начальной загрузки. Вредоносная программа использует адресацию логических блоков (*LBA*) для определения физического местоположения вредоносных данных на жестком диске [10].

FinSpy располагает широкими возможностями для слежки за пользователями. Так, версии зловреда для персонального компьютера могут:

- включать микрофон и записывать или транслировать злоумышленникам все, что он слышит;
- записывать или передавать злоумышленникам в реальном времени все, что пользователь вводит на клавиатуре;
- включать камеру и записывать или транслировать изображение с нее;
- копировать файлы, которые пользователь изменяет, отправляет на печать, получает, удаляет и так далее;
- снимать скриншоты или захватывать участок экрана там, где пользователь кликает мышью;
- воровать письма клиентов из *Thunderbird, Outlook, Apple Mail* и *Icedove*;
- перехватывать контакты, чаты, звонки и файлы в *Skype*.

В дополнение к этому версия *FinSpy* для ОС *Windows* может перехватывать *VoIP*-звонки, перехватывать сертификаты и ключи шифрования для определенных протоколов, а также загружать и запускать утилиты для сбора криминалистических данных. Помимо вышеперечисленного, *Windows*-версия шпиона способна заражать смартфоны.

Мобильные версии *FinSpy* могут прослушивать и записывать звонки – как голосовые, так и *VoIP*, читать *SMS* и следить за активностью пользователя в мессенджерах, таких как *WhatsApp, WeChat, Viber, Skype, Line, Telegram, Signal* и *Threema*. Кроме того, мобильный шпион отправляет злоумышленникам список контактов и звонков жертвы, мероприятия из календаря, информацию о местоположении устройства и многое др. [9].

***Remote Control System* (*RCS*) (*Hacking Team*, Италия)**

Hacking Team, также известная как *HT S.r.l.*, является компанией, расположенной в г. Милан, которая позиционирует себя как первую, предложившую наступательное решение для киберрасследований. Ее флагманский продукт *Remote Control System* (*RCS*), названный «хакерский пакет для правительственного перехвата», представляет собой набор имплантатов удаленного мониторинга (т.е. шпионских программ), продаваемых исключительно правительственным учреждениям по всему миру.

Remote Control System отличает от традиционных решений для наблюдения (например, прослушивания телефонных разговоров) возможность захватывать

данные, хранящиеся на компьютере цели, даже если цель никогда не отправляет информацию через интернет. *Remote Control System* также позволяет правительству следить за зашифрованными интернет-коммуникациями объекта, даже если объект подключен к сети, которую правительство не может прослушивать. Возможности *RCS* включают в себя копирование файлов с жесткого диска компьютера, запись звонков по *Skype*, мониторинг электронной почты, мгновенных сообщений и паролей, вводимых в веб-браузере. Кроме того, *RCS* может включать веб-камеру и микрофон устройства, чтобы следить за объектом [11].

На рис.1 представлена логическая архитектура прототипа развертывания *RCS Hacking Team*. В определенных случаях может использоваться «распределенная» архитектура.

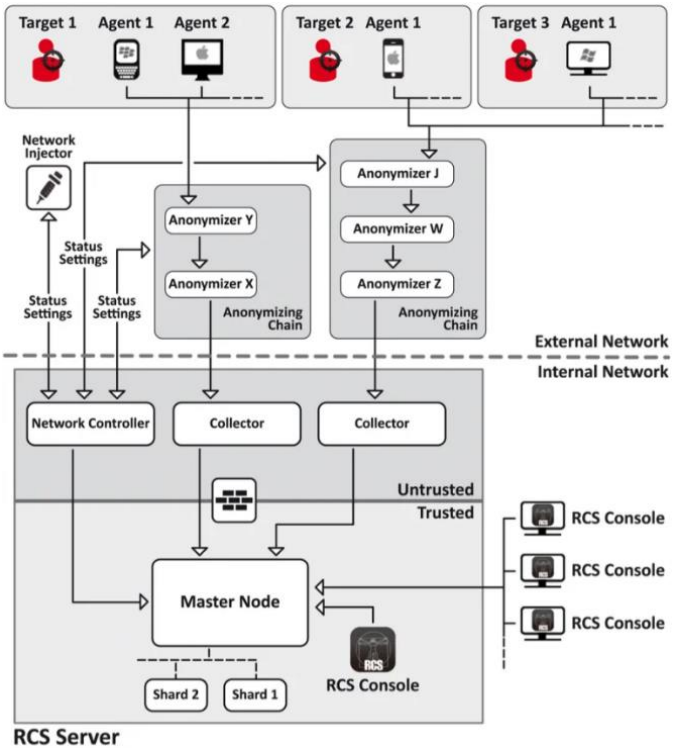

Рисунок 1

Remote Control System имеет ряд определенных ролей, каждая со своими собственными обязанностями и разрешениями в системе.

Системный администратор проходит обучение в *Hacking Team* на «этапе заключения контракта», а также выполняет другие задачи системного администрирования, включая установку и обновление серверов *RCS*, а также сетевых инжекторов.

Администратор создает учетные записи, выполняет операции и назначает цели.

Технический специалист отвечает за создание имплантатов (в документации они называются «агентами») и управление сетевыми инжекторами.

Аналитики обрабатывают выходные данные системы и выполняют интеллектуальный анализ с помощью консоли *RCS* [12].

***Predator* (*Cytrox*, Северная Македония)**

Predator – это шпионское ПО, разработанное компанией *Cytrox* и предназначенное для ОС *Android* и *iOS*. В мае 2022 г. исследователи из группы анализа угроз *Google* (*TAG*) сообщили, что *Predator* объединил пять эксплойтов

нулевого дня в один пакет и продал его нескольким субъектам, поддерживаемым правительством, которые использовали его в трех отдельных кампаниях. По словам исследователей, *Predator* тесно сотрудничал с компонентом под названием *Alien*, который «живет внутри нескольких привилегированных процессов и получает команды от *Predator*».

Анализ шпионского ПО, проведенный *Cisco Talos* в мае 2023 г., показал, что компонент *Alien* шпионского ПО активно реализует низкоуровневую функциональность, необходимую *Predator* для наблюдения за своими целями вместо того, чтобы просто выполнять функции загрузчика для *Predator*, как предполагалось ранее. В примере *Talos Alien* использовал пять уязвимостей, четыре из которых затрагивали *Google Chrome*, а последняя – *Linux* и *Android*, для заражения целевых устройств. После заражения устройства *Predator* получает полный доступ к его микрофону, камере и пользовательским данным, таким как контакты и текстовые сообщения. Кроме того, *Predator* имеет доступ к службам определения местоположения устройства и приложениям для обмена сообщениями, таким как *WhatsApp, Telegram* и *Signal*, что позволяет хакерам перехватывать и фальсифицировать сообщения [13].

***Hermit* (*RCS Lab*, Италия)**

Hermit – это шпионское ПО, разработанное итальянским коммерческим поставщиком шпионских программ *RCS Lab*, которое может быть тайно установлено на мобильные телефоны под управлением *iOS* и *Android.*

Компания *RCS Lab* занимается тем же бизнесом, что и *NSO Group*, которая получила известность благодаря своему шпионскому ПО *Pegasus* и продает шпионский софт правительственным учреждениям. Подобно *Pegasus, Hermit* способен отслеживать звонки, отслеживать местоположение, читать текстовые сообщения, получать доступ к фотографиям, записывать аудио, совершать и перехватывать телефонные звонки и способен получить *root* на устройствах *Android.* Некоторые злоумышленники выдавали себя за оператора мобильной связи жертвы, чтобы обманом заставить жертву загрузить приложение, которое доставит полезную нагрузку. Также вредонос выдавал себя за законное приложение для обмена сообщениями. Хотя приложения, содержащие шпионское ПО, не были доступны в *iOS App Store* или *Google Play Store*, злоумышленники смогли получить сертификаты, разрешающие установку зловреда на любое устройство *iOS*, через корпоративную программу *Apple* для разработчиков. Как только информация о *Hermit* стала достоянием общественности, *Apple* заявила, что отозвала связанные с ней сертификаты, а *Google* заявил, что распространил обновления *Google Play Protect* для всех пользователей [14].

***Regin* (АНБ, США)**

Regin (также известный как *Prax* или *QWERTY*) – это сложное вредоносное ПО и набор инструментов для взлома, используемый Агентством национальной безопасности США и его британским аналогом, Штаб-квартирой правительственных коммуникаций (*GCHQ*). Впервые оно была публично раскрыто «Лабораторией Касперского», «*Symantec*» и «*The Intercept*» в ноябре 2014 г. Вредоносная программа нацелена на конкретных пользователей компьютеров под управлением ОС *Windows* и была связана с агентством по сбору разведывательной информации АНБ США и его британским аналогом *GCHQ*. «The *Intercept*» предоставил образцы *Regin* для скачивания, включая вредоносное ПО, обнаруженное у бельгийского телекоммуникационного провайдера *Belgacom*. «Лаборатория Касперского» заявляет, что впервые узнала о *Regin* весной 2012 г.,

но некоторые из самых ранних образцов датируются 2003 г. (Имя *Regin* впервые было упомянуто на веб-сайте *VirusTotal* 9 марта 2011 г.) Среди компьютеров, зараженных Regin по всему миру, 28% находились в России, 24% – в Саудовской Аравии, по 9% – в Мексике и Ирландии и по 5% – в Индии, Афганистане, Иране, Бельгии, Австрии и Пакистане.

Regin использует модульный подход, позволяющий загружать функции, которые точно соответствуют цели, обеспечивая индивидуальную слежку. Конструкция делает его очень подходящим для постоянных, долгосрочных операций массового наблюдения за целями. Этапы развертывания вредоносного ПО *Regin* показаны на рис. 2.

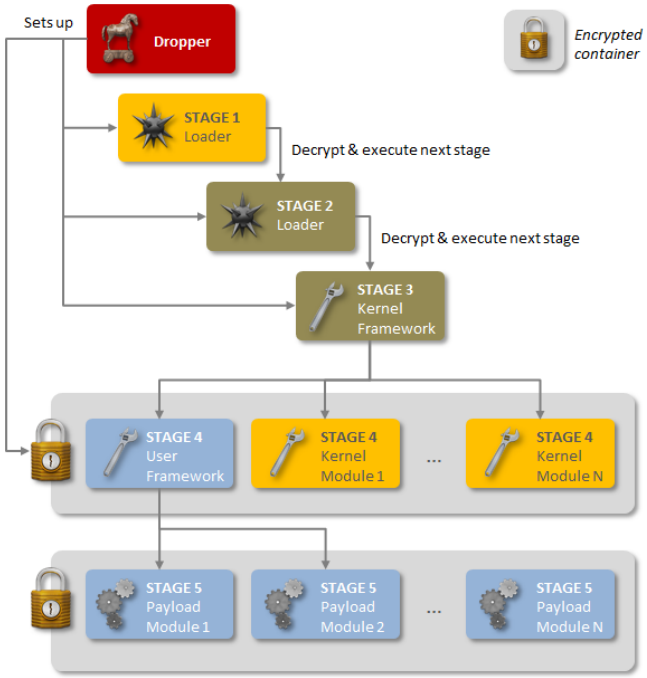

Рисунок 2

Regin работает скрытно и не хранит несколько файлов в зараженной системе; вместо этого он использует свою собственную зашифрованную виртуальную файловую систему (*EVFS*), которая использует вариант шифрования редко используемого шифра *RC*5. *Regin* взаимодействует через интернет, используя *ICMP/ping*, команды, встроенные в *HTTP cookies*, и пользовательские протоколы *TCP* и *UDP*, с сервером управления, который может контролировать операции, загружать дополнительные полезные данные и т.д. [15].

Сравнительный анализ различного вредоносного программного обеспечения

Проведем сравнительный анализ вредоносного ПО, применяемого правоохранительными органами различных стран при осуществлении оперативно-разыскной деятельности. Сравнительный анализ проводится по следующим критериям: страна происхождения, компания-разработчик, целевые устройства и ОС, эксплуатируемые уязвимости, эксплойты, ключевое воздействие, технические возможности, пути заражения.

Pegasus.
Страна происхождения: Израиль.
Компания-разработчик: *NSO Group*.

Целевыми объектами являются устройства с мобильными ОС *Android и iOS*.

Используются уязвимости *iOS CVE*-2016-4655, *CVE*-2016-4656, *CVE*-2016-4657, эксплойты *FORCEDENTRY, Zero-click* и др.

Ключевой особенностью является джейлбрейк *iPhone* или получение *root*-доступа *Android*-устройства.

Среди возможностей: анализ контактов, журналов вызовов, сообщений, фотографий, истории посещенных веб-страниц, настроек, прослушивание зашифрованных аудиопотоков и чтения зашифрованных сообщений, создания скриншотов, регистрации нажатия клавиш, а также сбора информации из приложений, включая, но не ограничиваясь ими, *Facebook, WhatsApp, iMessage, Gmail, Viber, Facebook, Telegram* и *Skype.*

Путей заражения несколько: фишинг, телефонный звонок (вне зависимости от того, будет ли ответ на звонок или нет), сообщения в *iPhone iMessage*, осуществление сетевой атаки.

FinSpy (FinFisher).

Страна происхождения: Германия.

Компания-разработчик: *Vilicius Holding GmbH.*

Целевыми объектами являются устройства с ОС *Windows, macOS* и *Linux* и мобильные устройства с *Android* и *iOS*.

Используются уязвимости в системе безопасности *iTunes* от *Apple* и др.

Ключевой особенность является загрузка и установка троянизированного приложения, выполняющего зловредные функции.

Среди возможностей: прослушивание и запись звонков, чтение *SMS* и слежка за активностью пользователя в мессенджерах, таких как *WhatsApp, WeChat, Viber, Skype, Line, Telegram, Signal* и *Threema*, извлечение списка контактов и звонков, мероприятий из календаря, информации о местоположении устройства и др.

Путей заражения несколько: запуск установщиков легальных приложений, в которых внедрен *FinSpy* (*TeamViewer, VLC Media Player, WinRAR* и др.), проникновение в загрузочную запись *UEFI* и *MBR* и фишинг (например, в *SMS*).

Remote Control System (RCS).

Страна происхождения: Италия.

Компания-разработчик: *Hacking Team.*

Целевыми объектами являются устройства с ОС *Android, BlackBerry, Apple iOS, Linux, Mac OS X, Symbian, Microsoft Windows, Windows Mobile* и *Windows Phone.*

Используется несколько эксплойтов: *Adobe Flash* в документе *Word, RTF*-файл с расширением *DOC* (*CVE*-2010-3333), переполнение целых чисел *Adobe Flash* «*Matrix*3*D*», *CVE*-2013-5331, *CVE*-2013-0633, *CVE*-2012-5054.

Ключевой особенностью является использование технологии прокси-цепочек для анонимизации правоохранительных органов.

Среди возможностей: скрытый сбор электронных писем, текстовых сообщений, историй телефонных звонков и адресных книг, регистрация нажатий клавиш, раскрытие данных истории поиска и создание скриншотов, запись телефонных звонков, активация камеры телефона или компьютера, взлом *GPS* для отслеживания местоположения цели, заражение *UEFI BIOS* прошивки целевого компьютера руткитом, извлечение паролей *Wi-Fi* и др.

Путей заражения несколько: фишинг, открытие документа *Microsoft Word* или просмотр веб-страницы.

Predator.

Страна происхождения: Северная Македония.

Компания-разработчик: *Cytrox*.

Целевыми объектами являются устройства с мобильными ОС *Android* и *iOS*.

Используются следующие уязвимости: *CVE*-2021-37973, *CVE*-2021-37976, *CVE*-2021-38000, *CVE*-2021-38003 в *Chrome* и *CVE*-2021-1048 в *Android.*

Ключевой особенностью является совместная работа с программным компонентом *Alien*, которое настраивает низкоуровневые возможности, необходимые *Predator.*

Основными возможностями являются: получение полного доступа к микрофону, камере и данным пользователя, таким как контакты и текстовые сообщения. *Predator* имеет доступ к службам определения местоположения устройства и приложениям для обмена сообщениями, таким как *WhatsApp, Telegram* и *Signal.* Он также позволяет перехватывать и фальсифицировать сообщения.

Пути заражения неизвестны.

Hermit.

Страна происхождения: Италия.

Компания-разработчик: *RCS Lab*.

Целевыми объектами являются устройства с мобильными ОС *Android* и *iOS*.

Используемые эксплойты и уязвимости неизвестны.

Ключевой особенностью является модульность *Hermit.*

Основными возможностями являются: отслеживание звонков, местоположения, чтение текстовых сообщений, получение доступа к фотографиям, запись аудио, совершение и перехват телефонных звонков, получение *root*-прав на устройствах *Android.*

Известно несколько векторов заражения: фишинг, *SMS*-сообщения, маскировка под сайты и приложения телекоммуникационных компаний или производителей смартфонов.

Regin.

Страна происхождения: США.

Компания-разработчик: АНБ.

Целевыми объектами являются устройства с ОС *Microsoft Windows*, а также *GSM*-операторы.

Используются эксплойты нулевого дня в браузере, веб-эксплойты.

Ключевой особенностью является модульный подход, позволяющий загружать функции, которые точно соответствуют цели, и наличие собственной зашифрованной виртуальной файловой системы (*EVFS*).

Основными возможностями являются: извлечение конфиденциальной информации, такой как электронные письма и документы, а также компрометация операторов связи.

Пути заражения неизвестны.

Заключение

Результаты анализа методов, применяемых государствами для осуществления так называемого правительственного взлома, а также используемое ими ПО, показывает, что рассмотренная государственная деятельность имеет высокую степень деструктивного воздействия на информационные системы, программные продукты, аппаратные и программно-аппаратные устройства.

Применяемые методы требуют высокого уровня профессиональной подготовки всех участников, включенных в данную деятельность. Используемые при этом программные продукты имеют различное происхождение, пути внедрения и функционал. Любая ошибка в осуществлении правительственного взлома может привести к трагическим последствиям.

На основании вышеизложенного, предлагается проведение законодательного регулирования данной деятельности применительно как к Российской Федерации, так и в международном пространстве. Регуляторами в данном случае могут выступать такие международные организации, как Организация Объединенных Наций, Совет Европы, Содружество Независимых Государств, БРИКС и др. С одной стороны можно сказать, что вышеупомянутые действия со стороны правоохранительных органов нарушают права и свободы граждан. Однако стоит также учитывать обязательство правоохранительных органов обеспечивать безопасность граждан и государства. Законодательным органам стран предстоит ставить эти две точки зрения на «чаши весов» и разрабатывать процедуры и законы, обеспечивающие интересы всех сторон общества.

Литература

1. URL https://www.varonis.com/blog/government-hacking-exploits (дата обращения - январь 2024 г.).
2. URL https://aphilosopher.wordpress.com/2017/05/17/the-ethics-of-stockpiling-vulnerabilities (дата обращения - январь 2024 г.).
3. URL https://www.aclu.org/news/privacy-technology/us-government-malware-policy-puts-everyone-risk (дата обращения - январь 2024 г.).
4. URL https://amnesty.org.ru/ru/2015-08-21-MorganMarquis-Boire (дата обращения - январь 2024 г.).
5. Mayer J. Government Hacking // The Yale Law Journal, 2018. – № 3. – С. 570-662.
6. URL https://www.bu.edu/riscs/2021/05/03/abuse-resistant-government-backdoors (дата обращения - январь 2024 г.).
7. URL https://ru.wikipedia.org/wiki/Pegasus_(программное_обеспечение) (дата обращения - январь 2024 г.).
8. URL https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf (дата обращения - январь 2024 г.).
9. URL https://www.kaspersky.ru/blog/finspy-for-windows-macos-linux/31671 (дата обращения - январь 2024 г.).
10. URL https://securityintelligence.com/analysis-of-finfisher-bootkit (дата обращения - январь 2024 г.).
11. URL https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware (дата обращения - январь 2024 г.).
12. URL https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant (дата обращения - январь 2024 г.).
13. URL https://en.wikipedia.org/wiki/Cytrox#Predator (дата обращения - январь 2024 г.).
14. URL https://en.wikipedia.org/wiki/Hermit_(spyware) (дата обращения - январь 2024 г.).
15. URL https://en.wikipedia.org/wiki/Regin_(malware) (дата обращения - январь 2024 г.).

РОЛЬ СПУТНИКОВОЙ НАВИГАЦИИ В СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.Н. Максименко, *к.т.н., доцент, Московский технический университет связи и информатики, vladmaks@yandex.ru;*
К.Н. Елагина, *Московский технический университет связи и информатики, kristina.elagina@mail.ru.*

УДК 004.056

Аннотация. Навигация представляет собой особенный сервис, который может выполнять функцию базового информационного сервиса и вспомогательного сервиса информационной безопасности. Навигационно-информационные системы (НИС) представляют собой особый класс информационных систем, в которых функция навигации (определение местоположения мобильных пользователей) расширяет набор решаемых информационных задач и формирует отдельный класс задач. Однако, вместе с этим, НИС могут быть подвержены различным видам воздействий (угроз). Нарушения в работе навигационных сервисов могут привести к авариям и крупным катастрофам, что повлечет за собой значительные материальные и человеческие потери. Именно поэтому обеспечение информационной безопасности навигационных систем становится все более важным и требует серьезного внимания. Необходимо создание системы защиты от угроз и контроля ее работы, а также постоянное улучшение методов обнаружения и защиты от новых угроз.

Ключевые слова: спутниковые системы; спуфинг-атака; цифровая подпись; технология *MIMO*; малоресурсная криптография.

THE ROLE OF SATELLITE NAVIGATION IN THE INFORMATION SECURITY SYSTEM

Maksimenko Vladimir, *Ph.D., Associate Professor, Moscow Technical University of Communications and Informatics.*
Elagina Kristina, *Moscow Technical University of Communications and Informatics.*

Annotation. Navigation is a special service that can perform the function of a basic information service and an auxiliary service of information security. Navigation and information systems (*NIS*) are a special class of information systems in which the navigation function (determining the location of mobile users) expands the set of information tasks to be solved and forms a separate class of tasks. However, at the same time, navigation and information systems can be subject to various types of impacts (threats). Disruptions in the operation of navigation services can lead to accidents and major disasters, which will entail significant material and human losses. That is why ensuring the information security of navigation systems is becoming more and more important and requires serious attention. It is necessary to create a system of protection against threats and control its operation, as well as to constantly improve the methods of detection and protection against new threats.

Keywords: satellite systems; spoofing attack; digital signature; *MIMO* technology.

Введение

Разработка систем связи и навигации с использованием искусственных спутников земли началась в 60-х гг. двадцатого века с разработки самой гуманной

деятельности человека: поисково-спасательных операций на море. Это, очевидно, одна из древнейших проблем, полностью реализовать которую еще предстоит.

С середины семидесятых годов прошлого века совместными усилиями многих стран были начаты работы по разработке системы «Инмарсат» – международной космической системы связи и навигации для морского флота. Аналогичную систему с более широкими возможностями по навигационному управлению по исследованию океанов и атмосферы разрабатывали под названием «Сарсат» (*Sarsat – Satellit aided rescue*) – спасение с помощью спутников.

В настоящее время навигация используется во многих сферах жизни. Она помогает не только определять местоположение объектов и рассчитывать безопасные маршруты движения, но и обеспечивать безопасность в процессе передвижения. Сочетание навигационных космических технологий и беспроводных радиотелефонных сетей позволило решать задачи поисково-спасательных операций на суше. В настоящее время функционируют четыре глобальные *GPS* (США), *GLONASS* (Россия), *BeiDou* (Китай), *GALILEO* (Европейский союз) и две региональные (Япония и Индия) спутниковые навигационные системы. Практическое применение российской системы ГЛОНАСС реализовано для решения социальных задач экстренного реагирования при дорожно-транспортных происшествиях в информационно-навигационной системе «ЭРА ГЛОНАСС», информационных и диспетчерско-навигационных системах автомобильного транспорта [1].

Навигация представляет собой особенный сервис, который может выполнять функцию базового информационного сервиса и вспомогательного сервиса информационной безопасности [2]. НИС представляют собой особый класс информационных систем, в которых функция навигации (определение местоположения мобильных пользователей) расширяет набор решаемых информационных задач и формирует отдельный класс задач. Однако, вместе с этим, НИС могут быть подвержены различным видам воздействий (угроз). Нарушения в работе навигационных систем могут привести к авариям и крупным катастрофам, что повлечет за собой значительные материальные и человеческие потери [3].

Именно поэтому обеспечение безопасности навигационных систем становится все более важным и требует серьезного внимания. Необходимо создание системы защиты от угроз и контроля ее работы, а также постоянное улучшение методов обнаружения и защиты от новых угроз [4, 5].

Угрозы информационной безопасности спутниковым данным

Актуальность исследований инженерных методов проектирования защищенных НИС обусловлена необходимостью обеспечения безопасности и надежности функционирования различных систем, которые используются во многих сферах деятельности, включая государственную безопасность, транспорт, энергетику, здравоохранение и другие. Сложность НИС, большой разнородный коллектив разработчиков, сокращение времени проектирования, ошибки проекта и неполное тестирование требуют ответственного выбора методов и средств для проектирования НИС.

Подавление спутникового сигнала – самая простая, очевидная и действенная атака на приемник спутникового сигнала. Принцип атаки заключается в генерации шумоподобного сигнала на частотах передачи спутникового сигнала (обычно ~1200-1600 МГц) с уровнем, превышающим реальный сигнал. Такая атака довольно проста в реализации, поскольку уровень спутникового сигнала обычно

невысок (по причине большого расстояния и прохождения различных слоев атмосферы), а генерация «шума» не составляет большого труда [3].

Спуфинг-атаки (англ. *spoofing* – подмена) – вид атак, при которых с помощью специального устройства, работающего на частотах ГНСС, приемнику под видом истинных данных посылаются ложные с более высоким уровнем сигнала. Приемник начинает работать с более сильным сигналом и получает заведомо ложные данные [4].

Все ранее известные работы по данной теме, в основном, сосредоточены на простых атаках путем установки поддельного местоположения в целевом навигационном устройстве [5-7]. В других работах изучаются атаки *GPS* на системы в открытой среде (например, в небе/в воде) [8, 9], где простая подмена *GPS*-сигнала может незаметно управлять навигацией.

Возможные способы предотвращения атак

Рассмотрим возможные механизмы защиты, способные помочь защититься от спуфинг-атак. Всего можно выделить три таких механизма: шифрование спутниковых данных, цифровая подпись и использование алгоритмов обнаружения атак.

Известные сервисы информационной безопасности для компьютерных систем необходимо дополнить сервисом «навигация» при расширении информационных систем навигационной составляющей:

- Идентификация и аутентификация.
- Управление доступом.
- Протоколирование и аудит.
- Шифрование.
- Контроль целостности.
- Экранирование.
- Анализ защищенности.
- Обеспечение отказоустойчивости.
- Обеспечение безопасного восстановления.
- Туннелирование.
- Управление.
- Навигация.

Сервисы безопасности в общей архитектуре безопасности распределяются по следующим уровням мер защиты:

- Превентивные меры, препятствующие нарушениям информационной безопасности.
- Меры обнаружения нарушений.
- Локализующие меры, сужающие зону воздействия нарушений.
- Меры по выявлению нарушителя.
- Меры восстановления режима безопасности.

Классификация сервисов информационной безопасности по уровням мер защиты:

К превентивным мерам относятся:

- Идентификация и аутентификация.
- Управление доступом.
- Шифрование.
- Обеспечение отказоустойчивости.

- Обеспечение безопасного восстановления.
- Управление.
- Навигация.

К обнаружению нарушений относятся:
- Протоколирование и аудит.
- Контроль целостности.
- Анализ защищенности.
- Навигация.

К мерам локализации нарушений относятся:
- Экранирование.
- Обеспечение отказоустойчивости.
- Обеспечение безопасного восстановления.
- Туннелирование.

К мерам по выявлению нарушителя относятся:
- Протоколирование и аудит.
- Управление.
- Навигация.

К мерам восстановления режима безопасности относятся:
- Обеспечение отказоустойчивости.
- Обеспечение безопасного восстановления.

Сервис информационной безопасности «навигация» может быть использован на нескольких уровнях мер защиты.

Распространение объектно-ориентированного подхода на информационную безопасность

По мере эволюции компьютерных систем структура процесса проектирования претерпела несколько модификаций. ГОСТ 34.601-90 регламентирует блочно-иерархическое проектирование, при котором на каждой стадии детализируются блоки предыдущего уровня. В стандарте *ISO\IEC* 15288 предлагается рассматривать жизненный цикл информационной системы в виде набора циклически повторяющихся процессов. Недостатком перечисленных стандартов проектирования заключается в низком уровне автоматизации. Использование объектно-ориентированного подхода и использование компьютерных средств проектирования информационных систем и программных систем повышают уровень автоматизации и сокращают сроки разработки [5, 6].

Проектирование информационных услуг при использовании объектно-ориентированного подхода начинается с разработки модели вариантов использования (диаграммы прецедентов). Главный прецедент определяет основную цель информационной услуги. Вспомогательные прецеденты определяют требования, которые должны быть выполнены для достижения цели.

Обобщенная диаграмма прецедента услуги на основе определения местоположения приведена на рис. 1 [10]. Требования информационной безопасности на диаграмме представлены прецедентами авторизации и получение доступа к системе, реализующей информационную услугу. Предоставление услуги на базе определения местоположения связано отношением расширения между

базовым вариантом использования и другим вариантом использования, функциональное поведение которого задействуется базовым не всегда, а только при выполнении дополнительного условия – определения местоположения [10].

Расширение сервиса услуг определением местоположения пользователя формирует новый класс услуг, обязательным для которого является периодическое информирование приложения о местоположении.

Основную часть этих действий выполняет система мониторинга. Система мониторинга – это система, которая работает с большим количеством информации в реальном масштабе времени. Для снижения требований производительности системы мониторинга используют принцип декомпозиции по функциональному принципу, используя показатели: ресурсы, сервисы и услуги (приложения) [4, 5].

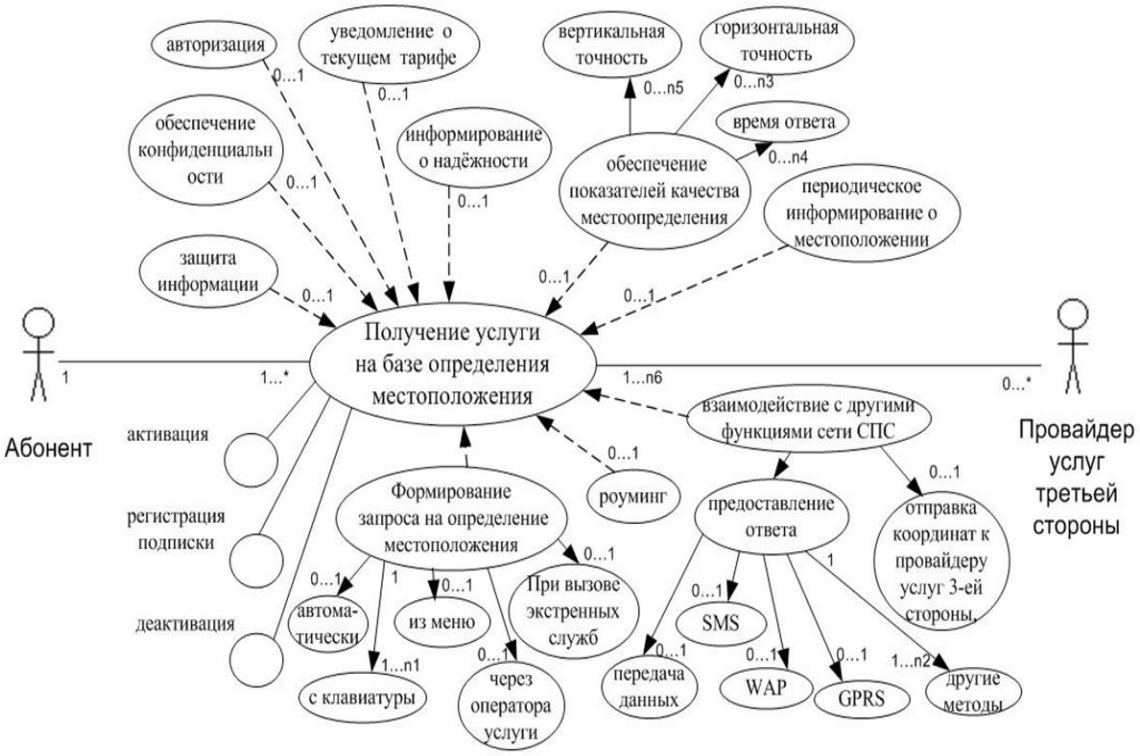

Рисунок 1

В рамках объектно-ориентированного подхода целью исследования является изучение моделей управления и качественных показателей навигационно-информационных систем. Предметом исследования являются инженерные методы проектирования навигационно-информационных систем [10].

Задачи, поставленные в работе:

1. Анализ навигационных технологий для проектирования навигационно-информационных систем.

2. Исследование формальных методов анализа расширенной модели управления инфотелекоммуникационной системой.

3. Исследование качественных показателей информационной безопасности на разных этапах жизненного цикла навигационно-информационных систем.

4. Разработка технологии проектирования защищенных навигационно-информационных систем с использованием компьютерных средств (CASE-технологии).

Для целей данного исследования воспользуемся следующим определением понятия «информационная безопасность» как защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных

воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Из данного определения следует, что существует два вида воздействий (угроз), первое – это случайные и естественные воздействия и второе – это преднамеренные и искусственные воздействия. Первые можно отнести к природным, не зависящим от человека воздействиям, а вторые – это угрозы, создаваемые человеком (злоумышленником). Защита от первого вида угроз может быть предусмотрена на ранних этапах жизненного цикла навигационно-информационной системы, а реагирование на угрозы злоумышленников возникают в основном на этапе эксплуатации жизненного цикла навигационно-информационной системы и решения по защите от данного вида угроз.

Был проведен сравнительный анализ трех наиболее распространённых технологий определения местоположения ГНСС, СПС и *WI-FI* и на основе показателей глобальности, точности и времени определения места положения была выбрана технология ГНСС для проектирования навигационно-информационных систем [1].

В настоящее время предпочтительным методом управления информационно-телекоммуникационными системами является ситуационный метод [3], базирующийся на непрерывном мониторинге информационной системы и оперативной реакции на нестандартные и непредвиденные ситуации. Ситуационный метод позволяет обеспечить защиту от искусственных и преднамеренных угроз, то есть от угроз, создаваемых злоумышленником. Это требует высокой квалификации оперативного персонала, что не всегда возможно. Поэтому предлагается разработать набор сценариев, которые позволили бы снизить требования к управляющему.

На этапе проектирования можем заложить сервисы безопасности ИБ от случайных и естественных угроз, такие как надежность, качество и устойчивость. Необходимо разрабатывать сервисы безопасности для этапа эксплуатации от преднамеренных воздействий искусственного характера. От второго типа угроз, которые создаются злоумышленниками, следует защищаться сервисами ИБ.

Выбор технологий для проектирования информационных систем с использованием компьютерных средств (*CASE*-технологии) имеет множество преимуществ:

Увеличение производительности. CASE-технологии сокращают время, затрачиваемое на разработку различных проектов, поскольку в них содержатся встроенные функции, которые значительно упрощают разработку и отладку кода.

Снижение затрат. Применение *CASE*-технологий снижает затраты на разработку информационных систем, за счет сокращения трудозатрат и скорости выполнения проектов.

Улучшение качества разработки. С помощью *CASE*-технологий можно разрабатывать сложные проекты с меньшим числом ошибок. Это достигается благодаря использованию готовых шаблонов, согласованных методик и процедур разработки, которые используются в *CASE*-средствах.

Улучшение коммуникации. CASE-технологии позволяют улучшить коммуникацию между разработчиками, дизайнерами, пользовательскими группами и другими членами команды, благодаря возможности создания единой документации проекта и облегчению взаимодействия между ними.

Увеличение гибкости и масштабируемости. CASE-технологии предоставляют гибкость и масштабируемость проектирования информационных

систем. Это позволяет быстро отвечать на изменения на рынке и в технических требованиях заказчика.

В целом, *CASE*-технологии являются существенным инструментом для разработки информационных систем и могут улучшить процесс проектирования и разработки, а также увеличить конечное качество продукта [4, 5, 10].

Концептуальная модель подсистемы информационной безопасности разработана на основе моделей *eTOM* и *SID*. Концептуальная модель подсистемы информационной безопасности приведена на рис. 2 и представлена в виде диаграммы классов в нотациях языка визуального моделирования *UML*. На диаграмме показаны классы и связи между ними. По диаграмме можно определить путь (сценарий) выбора контрмеры по угрозе и уязвимости.

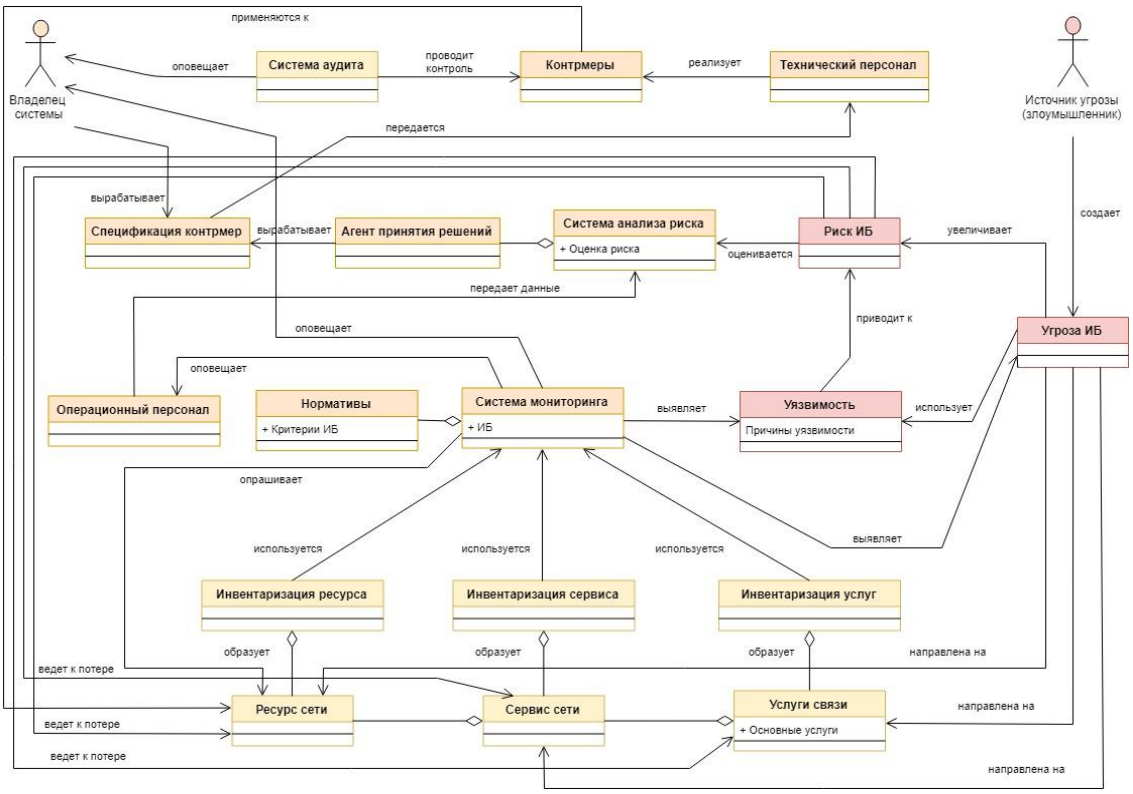

Рисунок 2

На концептуальной модели подсистемы информационной безопасности выделено три плоскости: угроз, уязвимостей и контрмер. Связи между тремя плоскостями составляют сценарий купирования от преднамеренных воздействий искусственного характера.

Архитектура безопасности должна обеспечивать защиту от угроз, будь то преднамеренные или случайные, такие как искажение или изменение информации, воровство, утечки, потери информации и других ресурсов, а также разглашение конфиденциальной информации.

Модель угроз может быть представлена при помощи диаграммы прецедентов. При помощи данной диаграммы можно определить на какую составляющую информационной безопасности направлена угроза: доступности, целостности, конфиденциальности или их сочетании.

На основе диаграмм прецедентов можно разработать сценарий ситуационного управления информационной безопасности информационной системы по одному объекту из классов (угроза, уязвимость, контрмера). Сценарий

позволяет по одной составляющей (угроза) разработать последовательность действий, которые могут привести к уязвимостям, связанным с данной угрозой, и выбрать соответствующую контрмеру.

Результаты данной работы имеют важное практическое значение. Исследование различных технологий позиционирования позволило выбрать оптимальную технологию ГНСС для использования в навигационно-информационных системах. Анализ формальных методов анализа расширенной модели управления инфотелекоммуникационной системой позволил определить подход, который будет эффективно применяться для управления системой. Исследование качественных показателей информационной безопасности на разных этапах жизненного цикла системы обеспечило понимание необходимых мер для защиты от угроз.

Заключение

Обобщая результаты работы, можно сделать вывод, что обеспечение безопасности навигационно-информационных систем является важной задачей, требующей комплексного подхода и постоянного совершенствования. Навигация представляет собой особенный сервис, который может выполнять функцию базового информационного сервиса и вспомогательного сервиса информационной безопасности [2]. Исследования и разработки, проведенные в рамках данной работы, позволяют принять меры по защите от угроз и обеспечить безопасность и надежность функционирования систем в различных областях навигационной деятельности.

Дальнейшие исследования в области НИС должны быть направлены на разработку новых методов и технологий, а также на адаптацию существующих подходов для эффективной борьбы с новыми угрозами. Также необходимо уделять внимание разработке и внедрению стандартов и нормативных документов, регулирующих безопасность навигационных систем. Это позволит обеспечить единый и стандартизованный подход к защите и управлению безопасностью в этой области.

Литература

1. Громаков Ю.А., Северин А.В., Шевцов В.А. «Технологии определения местоположения в GSM и UMTS». – М.: «Эко Трендз», 2005.
2. Максименко В.Н. Услуга определения местоположения абонента как средство защиты в сети сотовой подвижной связи // Известия ЮФУ, Технические науки. 2007. – № 4 (76). – С. 151-155.
3. Максименко В.Н., Ухин Д.А. Анализ уязвимостей каналов связи спутниковых навигационных систем LBS-услуги // Экономика и качество систем связи, 2019. – № 1 (11). – С. 18-22. – С. 37-41.
4. Максименко В.Н. Категорный подход к исследованию аспектов защиты информации и управления качеством сервисов и услуг в сетях сотовой подвижной связи // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 9. – С. 41-49.
5. Максименко В.Н. Конвергенция сервисов качества и защиты информации в сетях сотовой подвижной связи на этапах проектирования // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 11. – С. 57-64.
6. Крейнделин В.Б., Смирнов А.Э., Бен Режеб Т.Б.К. Эффективность методов обработки сигналов в системах MU-MIMO высоких порядков // T-Comm: телекоммуникации и транспорт, 2016. – Т. 10. – № 12. – С. 24-30.

7. Максименко В.Н., Васильев М.А. Методика расчета стандартных показателей качества дополнительных услуг на сетях подвижной связи // T-Comm: Телекоммуникации и транспорт, 2011. – Т. 5. – № 4. – С. 26-28.
8. Максименко В.Н., Васильев М.А. Методика системного проектирования инфокоммуникационных услуг сетей 3G // Электросвязь, 2011. – № 6.
9. Максименко В.Н., Соколов А.В. Цифровая подпись для защиты сигнала в структуре ГНСС // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 45-й международной конференции. Москва, 2020. – С. 28-31.
10. Леоненков А.В. Объектно-ориентированный анализ и проектирование с использованием UML и IBM Rational Rose: Учебное пособие / А.В. Леоненков. – М. Интернет-Университет Информационных Технологий, БИНОМ, Лаборатория знаний, 2010. – 320 с.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ФИЛЬТРАЦИИ ВРЕМЕННЫХ РЯДОВ ДЛЯ СОЗДАНИЯ ТОРГОВОГО БОТА

К.В. Портнов, *к.т.н., доцент, Самарский государственный технический университет, sk7@mail.ru.*

УДК 004.9

Аннотация. Статья посвящена разработке математического и алгоритмического обеспечения для торговых ботов на финансовых рынках с целью обеспечения автоматизации торговли на биржевых рынках и устранение эмоционального фактора при принятии решений. В качестве математического обеспечения выбраны механизмы цифровой фильтрации, позволяющие обеспечивать заданную вырезку области спектра входного сигнала или определенных частот для сглаживания незначительных (в контексте принятия решений) колебаний. Предложенные алгоритмы фильтрации нижних частот легли в основу создания программного фильтра, обрабатывающего временной ряд стоимости финансовых активов на биржах. Полученный фильтр используется для построения индикаторов разных порядков что позволяет использовать его при генерации торговых правил и сигналов в реверсивных или более сложных торговых системах.

Реализованный программный фильтр(индикатор) используется для создания системы торговых правил, на основании которых производится синтез алгоритма функционирования торгового бота. В настоящей работе указанный индикатор программно реализован в системе *Omega research* на встроенном языке программирования, хотя и в перспективе планируется разработка самостоятельного торгового бота, реализованного посредством среды *Lazarus IDE* и использование *API* библиотек *Meta Trader.*

Автором проведено экспериментальное оценивание использования реализованного алгоритма при проведении операций торговым алгоритмом торгового бота на исторических данных, представляющих собой временные ряды котировок различных финансовых активов. Указанное тестирование на разных финансовых инструментах проводилось автоматически с использованием встроенного функционала *Omega Research*, результаты которых приведены в статье.

Ключевые слова: биржевые роботы; цифровая фильтрация; дигитализация биржевого трейдинга; системный анализ процессов обработки сигналов; приоритетные направления цифровой трансформации; торговые роботы; торговые БОТы.

SOFTWARE IMPLEMENTATION OF A TIME SERIES FILTERING ALGORITHM FOR CREATING A TRADING BOT.

K.V. Portnov, *candidate of technical science, associate professor, Samara State Technical University.*

Annotation**.** The article is devoted to the development of mathematical and algorithmic support for trading bots in financial markets, with the aim of ensuring automation of trading in stock markets and eliminating the emotional factor in decision making. As mathematical support, digital filtering mechanisms were chosen to provide a specified cut of the spectral region of the input signal or certain frequencies to smooth out minor (in the context of decision-making) fluctuations. The proposed low-pass filtering algorithms formed the basis for the creation of a software filter that processes the time series of the value of financial assets on exchanges. The resulting filter is used to construct indicators of different orders, which allows it to be used when generating trading rules and signals in reverse or more complex trading systems.

The implemented software filter (indicator) is used to create a system of trading rules on the basis of which the algorithm for the functioning of the trading bot is synthesized. In this work, this indicator is implemented programmatically in the Omega research system using a built-in programming language, although in the future it is planned to develop an independent trading bot implemented through the Lazarus *IDE* and use the Meta Trader *API* libraries.

The author conducted an experimental evaluation of the use of the implemented algorithm when carrying out operations using the trading algorithm of a trading bot on historical data representing time series of quotes of various financial assets. The specified testing on various financial instruments was carried out automatically using the built-in functionality of Omega Research, the results of which are presented in the article.

Keywords: stock exchange robots; digital filtering, digitalization of stock trading; system analysis of signal processing processes; priority areas of digital transformation; trading robots; trading *BOTS*.

Введение

Цель работы – разработка математического, алгоритмического и программного обеспечения на основе цифровой фильтрации для проектирования торгового робота на финансовых рыках.

Разработка программного обеспечения сводится к двум частям - реализации алгоритма цифровой фильтрации, реализованного в форме самостоятельного временного ряда построенного на основе временного ряда финансового актива, и формированию на основе нескольких фильтров с разными параметрами сигналов принятия решений. Таким образом мы получаем систему с управляемыми параметрами.

В качестве математического аппарата были выбраны методы математико-статистического моделирования, а именно методы цифровой фильтрации сигналов. Под фильтром будем понимать произвольную систему обработки дискретного сигнала. Назначение фильтра – это извлечение или вырезка области спектра входного сигнала или определенной частоты.

Фильтрация осуществляется при помощи низкочастотного и высокочастотного фильтра. Низкочастотный фильтр предназначен для выделения тренда из исходных данных, т.е. низкочастотной составляющей временного ряда, а высокочастотный фильтр, наоборот, предназначен для устранения тренда.

Синтез алгоритма фильтрации

Временные ряды, которые интересуют нас в первую очередь – это динамика изменения курсов валют и акций. Обычно временной ряд содержит значения через равные промежутки времени. Этот промежуток времени называют периодом съема данных. Для курсов это может быть минута, час, день или даже месяц. Вообще говоря, динамику курсов принято характеризовать пятью величинами: цена открытия периода (*Open*), наибольшая цена за период (*High*), наименьшая цена за период (*Low*), цена закрытия периода (*Close*), объем операций за период, который может быть выражен в разных единицах, но в любом случае он характеризует активность рынка (*Volume*). Каждой из этих величин соответствует свой временной ряд, и даже более того, для каждой величины может быть несколько временных рядов в зависимости от выбранного периода съема данных.

Цифровые фильтры предназначены для обработки (фильтрации) сигналов, представленных в виде временных рядов. Одним из наиболее простых и полезных рекурсивных цифровых фильтров является фильтр Баттерворта. В данной работе остановимся на применении фильтра Баттерворта в трейдинге и методику построения торговой стратегии на созданных индикаторах. Широко известны два типа цифровых фильтров Баттерворта: синусный фильтр Баттерворда с базовым фильтром низких частот и тангенсный фильтр Баттерворда с базовым фильтром низких частот. По сравнению со своим аналоговым прототипом, синусный фильтр Баттерворда имеет более гладкие, а тангенсный фильтр – более крутые переходы от полосы пропускания к полосе поглощения фильтра.

В качестве базисного возьмем фильтр Баттерворта порядка 2p с передаточной функцией:

$$W_{2P}(S) = \prod_{k=1}^{P} \frac{1}{S^2 + 2 \cdot Cos\frac{(2k-1)\pi}{4P} \cdot S + 1} \quad (1)$$

где: S – оператор Лапласа.

Как видно из формулы 1, этот фильтр представляет собой *p* последовательно включенных колебательных звеньев.

Амплитудо-частотные и фазочастотные характеристики этого фильтра определяются по формулам 2:

$$\begin{cases} |W_{2p}(jx)| = \sqrt{\frac{1}{1+x^{4p}}} \\ \phi_{2p}(x) = \sum_{k=1}^{P} arctg \frac{2x\, cos\frac{(2k-1)\pi}{4p}}{1-x^2} \\ 0 \le x < 1 \\ \phi_{2p}(1) = p\frac{\pi}{2} \\ \phi_{2p}(x) = p\frac{\pi}{2} + \sum_{k=1}^{p} arctg \frac{x^2-1}{2x\, cos\frac{(2k-1)\pi}{4p}} \\ x > 1 \\ \phi_{2p}(x \to \infty) = p\pi \end{cases} \quad (2)$$

Здесь *x* – относительная частота; ω - круговая частота.

Алгоритм построения цифрового ФНЧ

Исходные данные: $\begin{cases} 2p - \text{порядок фильтра} \\ \Delta - \text{шаг дискретизации по времени} \\ \omega_{\text{в}} - \text{верхняя граничная частота фильтра} \end{cases}$

Системная функция цифрового ФНЧ получается из соотношения 1 путем замены параметра, указанного в формуле 3:

$$S = \frac{1}{tg\frac{\Delta\omega_{\text{в}}}{2}}\left(\frac{1-z^{-1}}{1+z^{-1}}\right) \tag{3}$$

где: *z*-1 – оператор запаздывания на один шаг дискретизации, в результате получаем вид передаточной функции, указанный в формуле 4:

$$W_{2p}(z) = \prod_{k=1}^{P} \frac{C_k(1+z^{-1})^2}{1-\lambda_1(k)z^{-1}+\lambda_2(k)z^{-2}} \tag{4}$$

Параметры фильтра вычисляются по формулам 5:

$$\left.\begin{cases} \lambda_1(k) = \dfrac{2\cos\Delta\cdot\omega_{\text{в}}}{1+cos\frac{(2k-1)\pi}{4p}\cdot sin\,\Delta\cdot\omega_{\text{в}}} \\ \lambda_2(k) = \dfrac{1-cos\frac{(2k-1)\pi}{4p}\cdot sin\,\Delta\cdot\omega_{\text{в}}}{1+cos\frac{(2k-1)\pi}{4p}\cdot sin\,\Delta\cdot\omega_{\text{в}}} \\ C_k = \dfrac{sin^2\frac{\Delta\cdot\omega_{\text{в}}}{2}}{1+cos\frac{(2k-1)\pi}{4p}\cdot sin\,\Delta\cdot\omega_{\text{в}}} = \dfrac{1-\lambda_1(k)+\lambda_2(k)}{4} \end{cases}\right\} k = \overline{1,p} \tag{5}$$

Частотные характеристики фильтра могут быть определены по соотношениям (2), если в них положить следующие значение *x* указанное формулой 6:

$$x = \frac{tg\frac{\Delta\cdot\omega}{2}}{tg\frac{\Delta\cdot\omega_{\text{в}}}{2}}; \tag{6}$$

где, $0 \le \omega \le \frac{\pi}{\Delta}$.

Алгоритм фильтрации временного ряда *Xm* (*m*=0, 1, …) описывается следующим рекурсивным соотношением 7:

$$\left.\begin{array}{l} Y_0(m) = x_m \\ Y_k(m) = \lambda_1(k)\cdot Y_k(m-1) - \lambda_2(k)\cdot Y_k(m-2) + \\ \qquad +C_k\{Y_{k-1}(m) + 2Y_{k-1}(m-1) + Y_{k-1}(m-2)\} \\ k = \overline{1,p} m = 0,\ 1,\ . .\ - \text{рекурсия} \\ Y_m = Y_p(m)\ - \text{выходной сигнал фильтра} \end{array}\right\} \tag{7}$$

Вычисления идут при условии, что $Yv(q)=0$ при $q<0$.

Для примера приводим алгоритм фильтрации для $P=3$ (шестой порядок фильтра). Он отражен в выражении 8:

$$\left.\begin{aligned} Y_1(m) &= \lambda_1(1)Y_1(m-1) - \lambda_2(1)Y_1(m-2) + C_1\{X_m + 2X_{m-1} + X_{m-2}\} \\ Y_2(m) &= \lambda_1(2)Y_2(m-1) - \lambda_2(2)Y_2(m-2) + C_2\{Y_1(m) + 2Y_1(m-1) + Y_1(m-2)\} \\ Y_3(m) &= \lambda_1(3)Y_3(m-1) - \lambda_2(3)Y_3(m-2) + C_3\{Y_2(m) + 2Y_2(m-1) + Y_2(m-2)\} \end{aligned}\right\} (8)$$

Программный индикатор реализован с помощью языка, встроенного в систему *Omega Research*:

```
{функция my_but_filter_N – ФНЧ Баттерворта}
inputs: price(numeric), p(numeric),T1(numeric);{цена, порядок фильтра, период отсечки}
vars: k(0),m(0),cow(0),siw(0),chet(true),CC(0),lam(0),tg(0);
arrays: cok[30](0),la1[30](0),la2[30](0),ck[30](0),y[30,3](close);
cow=cosine(360/T1); siw=sine(360/T1);
if floor(p/2)*2=p then chet=true
else chet=false; {проверка на четность порядка фильтра}
if chet then begin {если четный порядок, то...}
y[0,0]=price;
for k=1 to p begin
cok[k]=cosine((2*k-1)*180/4/p);
end;
end
else begin {если нечетный порядок, то...}
tg=tangent(180/T1);
lam=(1-tg)/(1+tg); CC=(1-lam)/2;
y[0,0]=lam*y[0,1]+CC*(price+price[1]);
for k=1 to p begin
cok[k]=cosine(k*180/(2*p+1));
end;
end;
{Общая часть}
for k=1 to p begin
la1[k] = 2*cow/(1+cok[k]*siw);
la2[k] = (1-cok[k]*siw)/(1+cok[k]*siw);
ck[k] = (1-la1[k]+la2[k])/4;
end;
{расчет выходного сигнала}
for k=1 to p begin
y[k,0]=la1[k]*y[k,1]-la2[k]*y[k,2]+ck[k]*(y[k-1,0]+2*y[k-1,1]+y[k-1,2]);
end;
{выход функции равен...}
my_but_filter_N=y[p,0];
{сдвигаем массив значений матрицы на 1 столбец – «забываем» самую старую историю}
for k=0 to p begin
for m=1 downto 0 begin
y[k,m+1]=y[k,m];
end;
```

```
end;
{текст индикатора butt_filer_N (без комментариев)}
inputs: price(c),p(2),T1(10),clrUp(red),clrDown(blue),clrNeutral(green);
value1=my_but_filter_N(price,p,T1);
value2=my_but_filter_N(price,p,T1)[1];
if value1 > value2 then plot1(value1,"",clrUp);
if value1 < value2 then plot1(value1,"",clrDown);
if value1 = value2 then plot1(value1,"",clrNeutral);
```

«Система» предполагает наличие исчерпывающего набора законченных правил, которые освобождают трейдера от необходимости самостоятельной интерпретации сигналов. Таким образом, торговая система представляет ничто иное, чем набор технических инструментов с определенными параметрами, которыми руководствуется трейдер при принятии решении, позволяя автоматизировать операции посредством использования сигналов и правил.

Создание торговой системы сводится не только к разработке математического аппарата, индикатора, фильтра. Важной стороной эффективной торговой системы будет являться разработка правил торговли, т.е. правила для открытия и закрытия позиций. Единственная задача, стоящая перед трейдером, будет настройка параметров торговой системы для конкретного рынка и тестирование, ее эффективности, на исторических данных.

Архитектура торгового робота схематично показана на рис. 1.

Рисунок 1

Этапы разработки торговой системы

Методы современного технического анализа позволяют существенно уменьшить риски трейдинга. Весь анализ может быть выполнен с использованием современных систем технического анализа *Omega Research, Metastock* и *Meta Trader.*

Необходимость автоматизации торговли на биржевых рынках вытекает как из необходимости получать котировки и управлять собственным счетом по каналам передачи данных, так из необходимости избежать субъективизма при принятии решения. Первые указанные причины достаточно просты в реализации и имеют большое количество качественных аналогов, представляющих собой

программные протоколы, с помощью которых создаются программные комплексы, предназначенные для управления счетом и получение котировок.

Более существенными причинами автоматизации трейдинга является проблема принятия решений. Компьютер, который на первых этапах использовался для быстрого поиска информации, для графической визуализации различных данных, для вычисления различных вспомогательных функций и т.п., теперь должен все больше брать на себя расчеты по выработке окончательных рекомендаций по принятию решений. Все этапы принятия решений, которые могут быть формализованы и которые не требуют выбора человека, необходимо передать компьютеру. При создании соответствующей программы человек получит возможность освободиться от рутинных расчетов и сконцентрироваться на проблеме выбора факторов, которые только он и может задавать. Разберем более подробно проблематику разработки подобных механических систем в следующей главе.

Для создания механической торговой системы были взяты фильтры нижних частот, входными данными которых помимо цены, являются порядок фильтра и период отсечки. В приложении приведен программный код фильтра для *Omega Research Tradestation*. Пересечение фильтров 2-го и 3-го порядка и периодом отсечки в 1 час изображено на рис. 2

Рисунок 2

Система носит реверсивный характер, т.е. сигналом на покупку и продажу служит пересечение двух фильтров (индикаторов). Хотя реверсивные системы на практике часто дают плохой результат, в данной работе хотим показать, что их стоит применять для торговли по тренду и применять либо для «бычьей», либо для «медвежьей» торговли. Для этого нами отдельно рассматриваются результаты общих торгов и результаты по коротким и длинным позициям.

Апробация торговой системы на исторических данных

Так как объем исторических данных достаточно велик, а расчеты, как правило, достаточно сложны, то трудно себе представить тестирование торговой

системы без использования программных средств. В связи с этим встает необходимость создания программного продукта в виде клиентского приложения, позволяющего не только производить расчеты с историческими и текущими данными и отображать их в привычном для трейдера виде, но и получать котировки через сеть интернет и производить торговые операции на рынке *FOREX*. Важная составляющая будет состоять в изучении предметной области и выборе эффективной торговой системы.

Экспериментальное исследование эффективности применения разработанного фильтра, лежащего в основе роботизированный торговой системы, проводилось на исторических данных, представляющих собой временные ряды котировок разных финансовых инструментов, соответствующих валютных пар за период 2002-2022 гг.

Для проведения исследования эффективности торговой системы был использован пакет *Omega Research Trade Station* 2000, позволяющий в автоматическом режиме проводить тестирование с изначально установленными параметрами (объем капитала, леверидж, порядки фильтров и т.п.), результаты которых приведены ниже.

В качестве исходных данных брались следующие величины:

- Инструмент: *JPY A0-FX/ CHF A0-FX/ EUR A0-FX/GBP A0-FX*
- Размер лота: 100 000
- Леверидж: 1/100
- Период: 60 мин
- Начальная дата: 15.01.02
- Конечная дата: 28.05.22

В ходе тестирования были построены графики динамики капитала. Динамика отражает результаты торгов по коротким и длинным позициям по каждой валютной паре.

Динамика капитала при тестовой торговле *EUR/USD* с помощью разработанной нами механической торговой системы изображена на рис. 3.

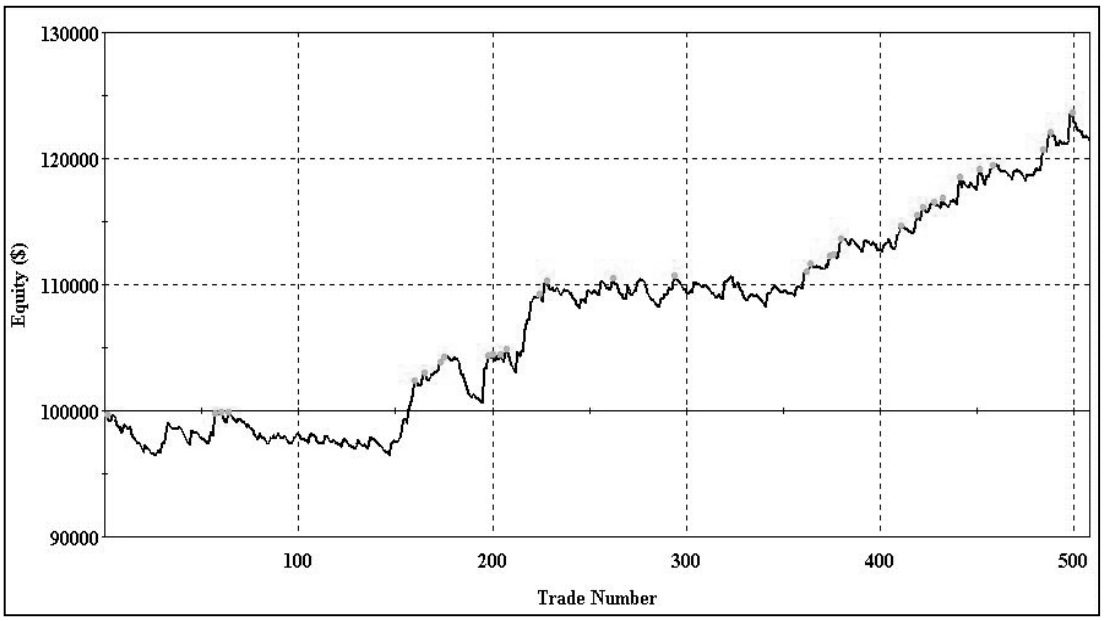

Рисунок 3

Динамика капитала при тестовой торговле *GBP* с помощью разработанной нами механической торговой системы изображена на рис. 4

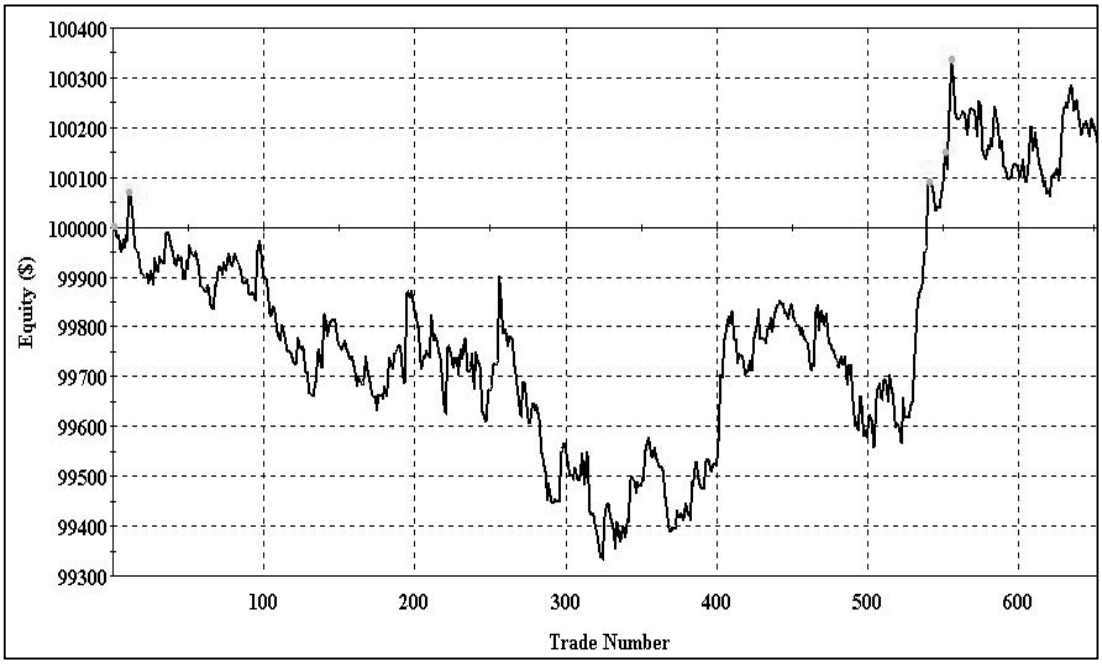

Рисунок 4

Динамика капитала при тестовой торговле *USD/CHF* с помощью разработанной нами механической торговой системы изображена на рис. 5

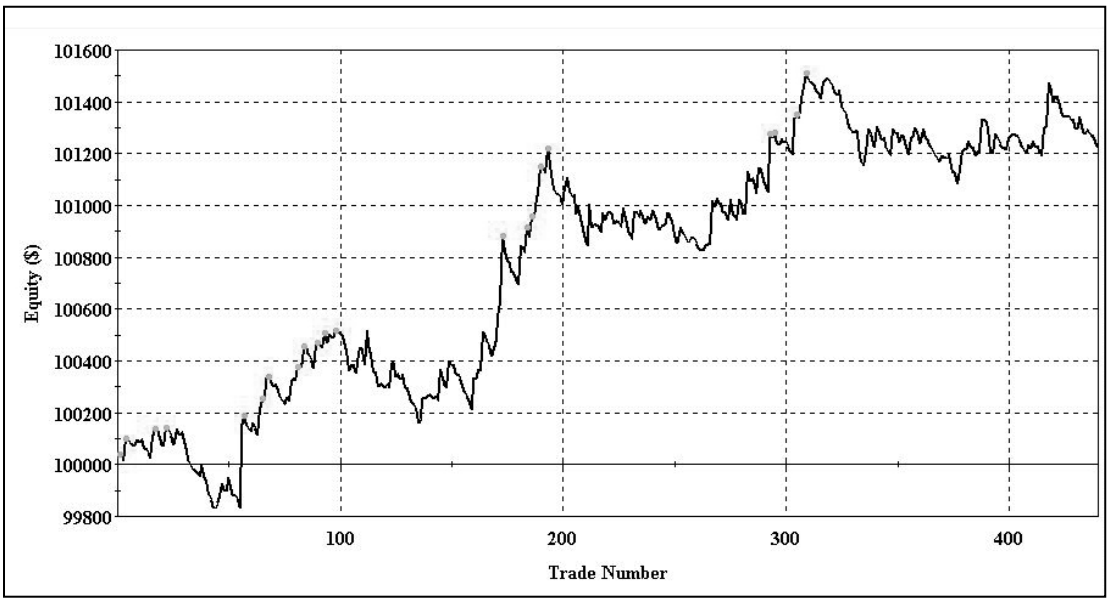

Рисунок 5

Динамика капитала при тестовой торговле *JPY* с помощью разработанной нами механической торговой системы изображена на рис. 6.

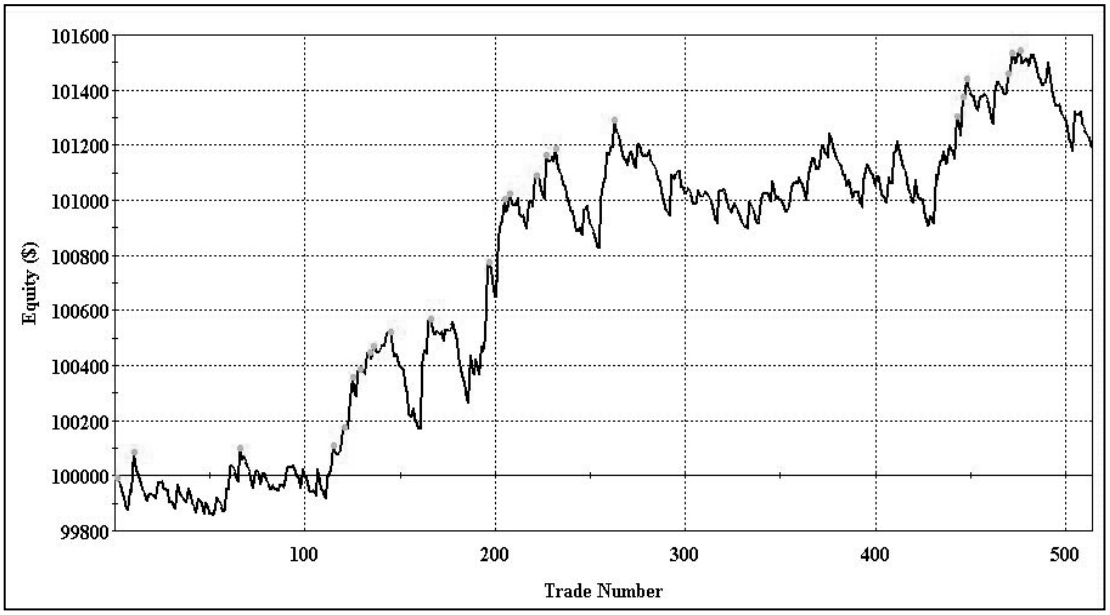

Рисунок 6

Детализированные финансовые результаты экспериментальных операций, проводимых на исторических данных, в целом отражены в табл. 1., а результаты по «длинным» и «коротким» позициям в табл. 2 и 3 соответственно.

Таблица 1.

Показатель	***EUR/USD***	***USD/CHF***	***USD/JPY***	***GBP/USD***
Общее количество сделок	508	514	440	658
Прибыльные сделки	204	193	162	284
Убыточные сделки	304	321	278	374
Процент прибыльных сделок	40,16%	37,55%	36,81%	43,16%
Наибольшая прибыль	$2721,12	$260,62	$317,25	$171,34
Наибольший убыток	$850,82	$74,03	$88,20	$96,26
Средняя прибыль	$428,27	$42,97	$46,15	$24,12
Средний убыток	$216,99	$22,12	$22,49	$17,99
Коэффициент среднего выигрыша/убытка	1,97	1,94	2,05	1,34
Валовая прибыль	$87366,18	$8292,83	$7475,79	$6848,94
Валовый убыток	$65965,62	$7099,38	$6251,38	$6727,86
Чистая прибыль	$21400,56	$1193,45	$1224,40	$121,08
Прибыльность стратегии	21,4%	1,19345%	1,22%	0,122%
Прибыльность (при использовании маржи)	2140,4%	119,345%	122%	12,2%

Таблица 2.

Показатель	***EUR/USD***	***USD/CHF***	***USD/JPY***	***GBP/USD***
Общее количество сделок	239	246	235	329
Прибыльные сделки	106	87	85	150
Убыточные сделки	133	159	150	179

Показатель	*EUR/USD*	*USD/CHF*	*USD/JPY*	*GBP/USD*
Процент прибыльных сделок	44,35%	35,37%	36,17%	45,59%
Наибольшая прибыль	$2721,12	$260,62	$252,45	$171,34
Наибольший убыток	$850,82	$74,03	$67,20	$51,29
Средняя прибыль	$520,11	$40,99	$40,20	$21,41
Средний убыток	$227,70	$23,69	$20,80	$14,64
Коэффициент среднего выигрыша/убытка	2,28	1,73	1,93	1,46
Валовая прибыль	$55131,32	$3566,39	$3416,94	$3211,16
Валовый убыток	$30283,94	$3766,97	$3122,05	$2621,71
Чистая прибыль	$24847,39	$-200,58	$294,89	$589,45
Прибыльность стратегии	24,85%	-0,2%	0,29489%	0,5895%
Прибыльность (при использовании маржи)	2485,4%	-20%	29,489%	59%

Таблица 3.

Показатель	*EUR/USD*	*USD/CHF*	*USD/JPY*	*GBP/USD*
Общее количество сделок	269	268	205	329
Прибыльные сделки	98	106	77	134
Убыточные сделки	171	162	128	195
Процент прибыльных сделок	36,43%	39,55%	37,56%	40,73%
Наибольшая прибыль	$2210,15	$233,60	$317,25	$168,67
Наибольший убыток	$783,78	$63,29	$88,20	$96,26
Средняя прибыль	$328,93	$44,59	$52,71	$27,15
Средний убыток	$208,66	$20,57	$24,45	$21,06
Коэффициент среднего выигрыша/убытка	1,58	2,17	2,16	1,29
Валовая прибыль	$32234,87	$4726,44	$4058,85	$3637,78
Валовый убыток	$35681,71	$3332,41	$3129,33	$4106,15
Чистая прибыль	-$3446,84	$1394,04	$929,52	$-468,38
Прибыльность стратегии	-3,4465%	1,3940%	0,9295%	-0,464%
Прибыльность (при использовании маржи)	-344,65%	139,40%	92,95%	-46,4%

В результате тестирования выяснилось, что наилучшие результаты торгов были получены для *EUR/USD* и составляет 21,4%, но т.к. на Форексе используется кредитное плечо (леверидж) 1/100, то прибыльность маржинальной торговли составляет 2140%. По остальным валютам были получены более плохие результаты. Это вполне нормальное явление, т.к. для каждой валюты следует подбирать индивидуальные комбинации порядков фильтра (индикатора), вследствие их характерных особенностей. Автоматизированный подбор порядков реализуется в специальных программных пакетах, позволяющих методом перебора добиться наилучшего финансового результата за данный временной период. Данную оптимизацию позволяют производить такие пакеты как *Omega Research Trade Station 2000i*. В разработанной нами автоматизированной информационной системе в дальнейшем планируется сделать возможность тестирования механических торговых систем и их оптимизацию.

Стоит отметить, что результаты тестирования будут отличаться от торговли в реальных условиях т.к. невозможно учесть психологическое состояние трейдера, а также эффекта проскальзывания. Необходимо учитывать и тот фактор, что сигнал механической торговой системы при тестировании формируется после завершения временного периода, на котором произошло выполнение условия входа в рынок, проще говоря, сигнал появляется после формирования свечи, на которой произошло выполнение условия. Следующий немаловажный фактор то, что торговля при тестировании ведется без установки *Stop-loss и take-profit,* и это ведет к достаточно существенной потенциальной возможности просадки капитала. Ну и последним неучтенным фактором является спрэд, который в реальных условиях тоже может повлиять на результаты торговли.

При тестировании лучшие результаты были получены по тем позициям, в направлении которой шел рынок. Например, результаты коротких позиций по *CHF* были намного лучше, чем по длинным и составили 139,5% прироста капитала. По длинным позициям был получен отрицательный результат, что снизило прибыльность механической торговой системы в целом.

Таким образом, мы рекомендуем использовать индикатор для торговли только по тренду в направлении рынка. Это позволит увеличить прибыльность и прирост капитала.

Заключение

Разработан алгоритм цифровой фильтрации для специализировнных программных комплексов типа *Meta Stock, Omega Research, Meta Trader,* обеспечивающий построение трендового индикатора на основе низкочастотной фильтрации для обеспечения поддержки принятия решения при операциях финансовых рынках.

Проведено исследование эффективности принятия решения на основе реализованных индикаторов на исторических данных, которое показало состоятельность данного метода в биржевом техническом анализе.

Разработанное программное обеспечение предназначено для работы биржевых трейдеров на валютном рынке Форекс.

Автоматизированная система реализована полностью и готова к внедрению. Для повышения эффективности рекомендуется произвести предварительную настройку периодов группы индикаторов Баттерворта для текущего рынка и для каждой валютной пары.

Литература

1. Портнов К.В. Анализ цифровой трансформации бизнес-процессов // Актуальные проблемы общества, экономики и права в контексте глобальных вызовов: Сборник материалов X Международной научно-практической конференции, Москва, 17 мая 2022 года / Редколлегия: Л.К. Гуриева [и др.]. – Москва: Общество с ограниченной ответственностью «ИРОК», ИП Овчинников Михаил Артурович (Типография Алеф), 2022. – С. 49-58. – DOI 10.34755/IROK.2022.92.13.091. – EDN EJPTQW.
2. Портнов К.В. Генетические алгоритмы и поиск эффективных порядков индикаторов в биржевой торговой стратегии на основе пересечения трех скользящих средних // Вестник Самарского государственного технического университета. Серия: Технические науки, 2005. – № 32. – С. 72-76. – EDN JWUXKZ.
3. Портнов К.В. Информационные технологии в оценке показателя лояльности клиентов // В мире научных открытий, 2011. – № 3 (15). – С. 254-258. – EDN OCSJNX.

4. Смагина З.А. Технология интернет вещей и ее влияние на современную экономику // Теоретические и прикладные вопросы экономики, управления и образования: Сборник статей II Международной научно-практической конференции. В 2-х томах, Пенза, 15-16 июня 2021 года. Том II. – Пенза: Пензенский государственный аграрный университет, 2021. – С. 182-186. – EDN AJTHBC.
5. Портнов К.В. Анализ задачи оценки лояльности в деятельности компаний в сфере профессиональных услуг // Проблемы развития предприятий: теория и практика, 2020. – № 1-2. – С. 241-244. – EDN HDSWOD.
6. Свидетельство о государственной регистрации программы для ЭВМ № 2023664735 Российская Федерация. Система учета товаров на складе интернет-магазина: № 2023660391: заявл. 24.05.2023: опубл. 06.07.2023 / К.В. Портнов; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный технический университет». – EDN VFHCBC.
7. Латушкина Т.С. Исследование возможностей интернет-продвижения и настройка рекламной компании // Московский экономический журнал, 2023. – Т. 8. – № 5. – DOI 10.55186/2413046X_2023_8_5_280. – EDN RFPBDO.
8. Сахбиева А.И., Калякина И.М., Косников С.Н., Латушкина Т.С., Майорова И.А. Цифровизация экономика и обеспечение безопасности данных // Московский экономический журнал, 2021. – № 8. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-8-2021-28
9. Иноземцев В.Л. На рубеже эпох. Экономические тенденции и их неэкономические следствия [Текст]. – М.: Экономика, 2003. – 730 с.
10. Латушкина Т.С., Харитонова Е.А., Майорова И.А. Анализ подходов к ESG на примере металлообрабатывающего предприятия // Экономика и предпринимательство, 2022. – № 7 (144). – С. 1059-1064.
11. Латушкина Т.С., Майорова И.А. Использование и применение JAVASCRIPT-фреймворков (REACT, ANGULAR, VUE.JS) для разработки WEB-приложений // Экономика и предпринимательство, 2023. – № 9 (158). – С. 1374-1376.
12. Портнов К.В. Актуальные проблемы и задачи автоматизированных систем в сфере ЖКХ // Журнал монетарной экономики и менеджмента, 2024. – № 2. – С. 230-236. – DOI 10.26118/2782-4586.2024.35.72.033. – EDN AEQRFJ.
13. Портнов К.В. Разработка информационной системы на основе многофакторной логистической регрессии // Информационные технологии. Радиоэлектроника. Телекоммуникации, 2012. – № 2-3. – С. 129-133. – EDN PEDEUX.
14. Портнов К.В. Анализ оценки неопределенности инвестиционного портфеля // Математическое моделирование и краевые задачи: Труды Третьей Всероссийской научной конференции, Самара, 29-31 мая 2006 года / Редколлегия: В.П. Радченко (ответственный редактор), Э.Я. Рапопорт, Е.Н. Огородников, М.Н. Саушкин (ответственный секретарь). Том Часть 4. – Самара: Самарский государственный технический университет, 2006. – С. 80-82. – EDN TGOHNF.

ПРИМЕНЕНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ ЗЛОУМЫШЛЕННИКАМИ ДЛЯ СКРЫТОГО ОБМЕНА ИНФОРМАЦИЕЙ И ОСУЩЕСТВЛЕНИЯ КОМПЬЮТЕРНЫХ АТАК

М.Ю. Федосенко, *Национальный исследовательский университет ИТМО, fedosenkomaksim98@gmail.com;*
А.В. Агарков, *Национальный исследовательский университет ИТМО, a1sk8te@yandex.ru.*

УДК 004.056

Аннотация. Сфера кибербезопасности непрерывно развивается, поскольку злоумышленники постоянно ищут новые и изощренные способы нарушения целостности, конфиденциальности и доступности систем и сетей. Одним из таких способов является применение методики сетевой стеганографии, при помощи которой скрытые данные передаются законными путями, с использованием легитимных сетевых соединений. В данной статье исследуются методы сетевой стеганографии, которые применяются для передачи и вложения стеганограммы в сетевые пакеты.

Ключевые слова: сетевая стеганография; сети; сетевые протоколы; скрытая передача данных; *TCP/IP*.

APPLICATION OF NETWORK STEGANOGRAPHY BY CRIMINALS FOR HIDDEN INFORMATION EXCHANGE AND IMPLEMENTATION OF COMPUTER ATTACKS

M. Fedosenko, *National Research University ITMO;*
A. Agarkov, *National Research University ITMO.*

Annotation**.** The cybersecurity is constantly evolving because attackers continually seek new and sophisticated ways to compromise the integrity, confidentiality, and availability of systems and networks. One such method is the use of network steganography techniques, in which hidden data is transmitted to legitimate ways, using network connections. This paper contains network steganography methods that are used to transmit and embed steganograms in network packets.

Keywords: network steganography; networks; network protocols; hidden data transmission; *TCP/IP*.

Введение

Сетевая стеганография – это методика, которая используется злоумышленниками для скрытого обмена информацией, позволяющая спрятать данные внутри обычных, часто используемых легальных сетевых соединений. Такая концепция скрытой передачи делает передачу данных почти невидимой для систем безопасности. Важно, чтобы отправитель и получатель знали о процессе стеганографии, поскольку для стороннего наблюдателя такая передача данных является вполне законной, даже при неглубоком анализе трафика. Информация, вложенная в полезную нагрузку пакета и передаваемая с помощью стеганографии, называется стеганограммой. Процедура, которая анализирует пакеты в сетевом трафике на обнаружение стеганографии и наличия стеганограмм называется стегоанализом.

Сетевой пакет, это основной юнит, используемый для передачи данных по сети. Он представляет из себя контейнер, содержащий передаваемую информацию от одного устройства в сети к другому. Независимо от использования протокола

сетевой пакет может содержать основные поля, например, поле заголовка, полезной нагрузки, адреса отправителя и адреса получателя и т.д. Некоторые из этих полей могут включать полезную информацию, передаваемую при обмене пакетами между системами. Кроме этого, пакеты могут разбиваться, т.е. фрагментироваться, в зависимости от используемого протокола. Это позволяет не превышать размер ограничения *MTU* (максимальная единица передачи), не вызывая тем самым ограничения пропускной способности сети, и потерю пакетов, которая приводит к задержке и потери данных.

Такую архитектуру передачи данных по сети активно используют злоумышленники, чтобы передавать скрытые данные в легитимных пакетах. Согласно *MITRE ATTACK* [1] сетевая стеганография относится к классу обфускации данных под идентификатором T1001.002 и включает в себя 11 техник, применяемых для передачи стеганограммы по сети.

Целью данного исследования является рассмотрение различных методов вложения и передачи стеганографической информации с помощью сетевого трафика, а также установление особенностей изменения сетевых пакетов для последующей реализации механизмов защиты сетевой инфраструктуры от скрытых атак, реализованных посредством вредоносных вложений в пакеты.

Реализация поставленной проблемы предполагает следующие задачи:

- Классификация методов сетевой стеганографии в зависимости от механизмов сокрытия данных внутри трафика.
- Литературный анализ научных работ по исследуемой тематики с целью выделения и обобщения случаев и особенностей практического применения сетевой стеганографии.
- Определение сетевых протоколов модели *OSI*, позволяющих сокрытие данных и степени возможностей практического осуществления сокрытия и последующего обмена стеганографией.
- Сравнительный анализ полученных методов.

Методы сетевой стеганографии

В целом методы сетевой стеганографии можно разделить на три большие группы:

- Методы, изменяющие данные в полях заголовков сетевых протоколов.
- Методы, изменяющие структуру передачи сетевых пакетов.
- Гибридные методы, основанные на изменении содержимых пакетов, структуру передачи и сроков доставки.

В работе [2] исследуется метод вставки секретных данных в фрагменты пакета на основе идентифицирующей последовательности (*IS*). Идентифицирующая последовательность в данном методе применяется для того, чтобы различать стеганографические фрагменты от обычных, увеличивая сложность обнаружения таких фрагментов. При этом *IS* содержит дополнительные значения смещения фрагмента и номер идентификации фрагмента. Идентифицирующая последовательность заранее составляется с помощью хэш-функции отправителем и получателем. Далее, передача стеганограммы принимает следующий вид:

1. Отправитель добавляет секретные данные в полезную нагрузку фрагмента *IP*-пакета.

2. Вычисляется *IS* с помощью хэш-функции с заранее известным *Steg*-ключом и добавляется в полезную нагрузку фрагмента.

3. На принимающей стороне на основе значения *Steg*-ключа вычисляется *IS*.

4. Пакет извлекается, если *IS* в его полезной нагрузке совпадает с вычисленной на предыдущем этапе.

Значения в полях смещения фрагмента и идентификации остаются такими же, как и в других допустимых фрагментах. Пример метода изменения фрагментов представлен на рис. 1 (*H* – заголовок, *P* – полезная нагрузка, *S* – секретные данные), где: *Steganography Sender* (*SS*) является отправителем стеганограммы и источником фрагментации, а *Recipient of Steganography* (*SR*) получателем.

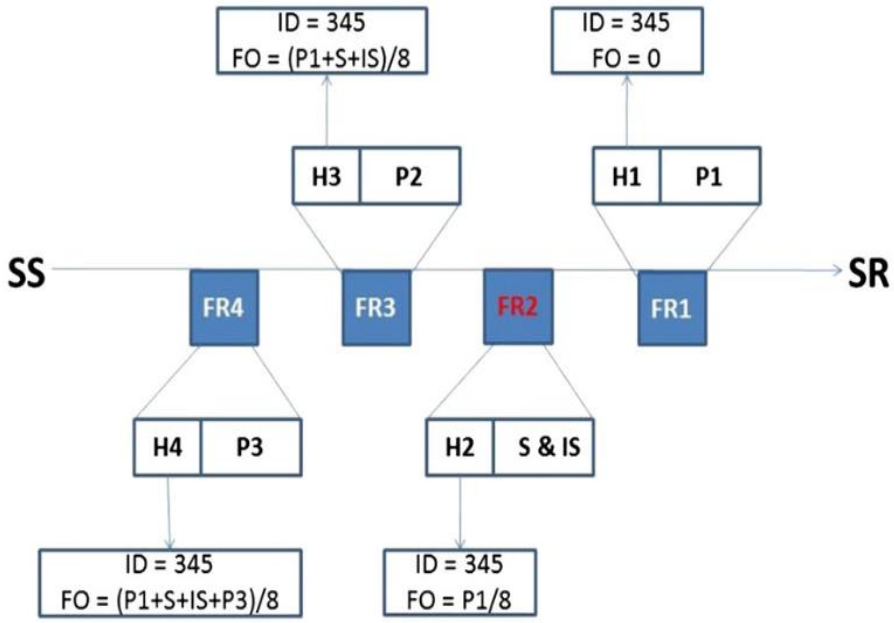

Рисунок 1

Помимо метода изменения фрагмента, в работе [2] авторы приводят пример метода модуляции числа фрагментов, который основан на изменении структуры передачи пакетов путем вставки скрытого бита. *SS* добавляет один бит данных, разделяя, таким образом, каждый из *IP*-пакетов на предопределенное количество фрагментов. В зависимости от ранее обговоренного способа обнаружения стеганографии *SR* может считывать передаваемую стеганограмму, как показано на рис. 2.

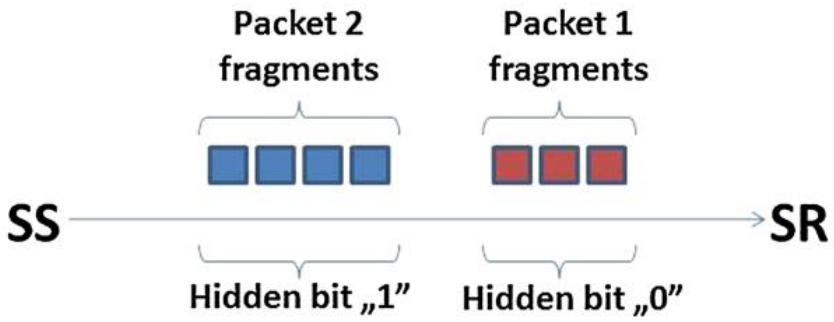

Рисунок 2

Алгоритм работы данного метода следующий:

1. Отправитель разбивает *IP*-пакет на множество фрагментов.
2. Четное количество фрагментов означает передачу двоичного «0».

3. Нечетное количество фрагментов означает передачу двоичной «1».

4. Извлечение данных из трафика основано на заранее обговоренном количестве пакетов.

В работе [3] также рассматривается этот метод, недостатком которого является ограниченное количество информации, передаваемой таким образом и легкость в обнаружении. Однако, авторы работы [2] предлагают решение проблем, связанных с использованием этого метода путем объединения с методом изменения фрагментов и применения их одновременно к общему носителю, в виде сетевого протокола.

В работе [4] исследуется гибридный метод стеганографии, который включает в себя изменение сетевого пакета и структуры передачи пакетов. Метод основан на принудительной потере пакетов *Lost Audio Packets* (*LACK*) и используется в технологиях телефонии, например, *VoIP* при передаче пакетов протокола *Real-time Transport Protocol* (*RTP*). Принцип работы данного метода, следующий:

1. Выбирается один пакет *RTP* из голосового потока.
2. Полезная нагрузка выбранного *RTP*-пакета заменяется секретным сообщением.
3. Выбранный пакет намеренно задерживается перед передачей.
4. Пакет распознается как чрезмерно задержанный и извлекается стеганограмма.

SS намеренно задерживает некоторые выбранные *RTP*-аудиопакеты перед передачей. Пакеты отбрасываются на стороне *SR*, если задержка таких пакетов в приемнике считается чрезмерной, а также отбрасываются в том случае, если получатель не осведомлен о процедуре стеганографии. Голосовая полезная нагрузка фрагмента заменяется битами стеганограммы в соответствии, например, с методом на основе изменения фрагмента, как показано на рис. 3.

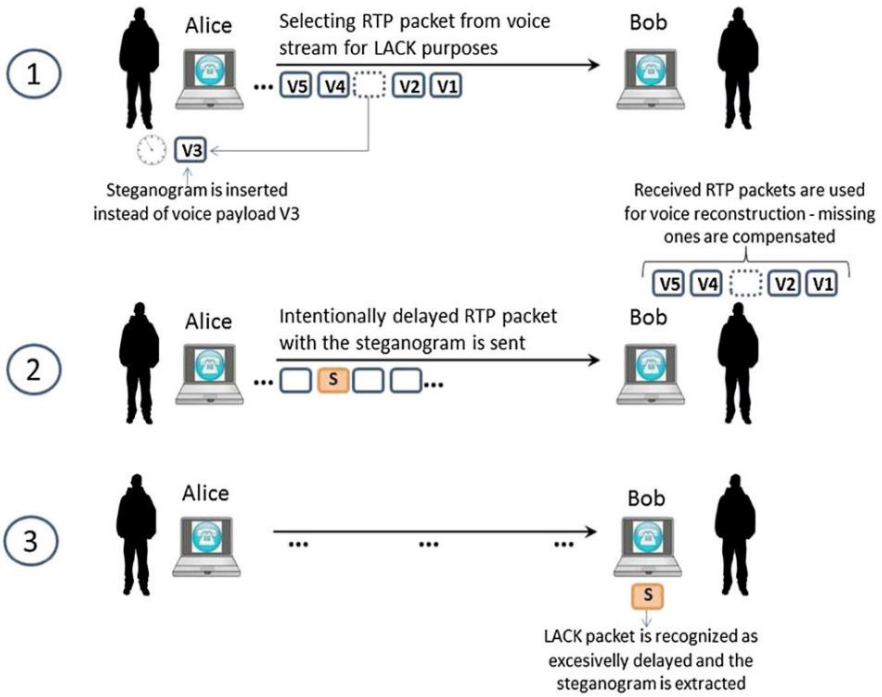

Рисунок 3

Однако, данный метод имеет недостатки, связанные с качеством передаваемой информации, которая ухудшится, если будет задержано слишком много *RTP*-пакетов, в результате этого выполнение стеганоанализа будет тривиальным. Как сообщают авторы исследования [3], данный метод обладает средней сложностью обнаружения и имеет сложную реализацию, зависящую от определенных операционных систем.

Как показывают авторы [2], метод можно улучшить при соблюдении осторожности во время выбора *RTP*-пакетов. В целях уменьшения общего уровня потери пакетов и в соответствии с условиями сети, высока вероятность не достигать определенного порога обнаружения.

В качестве меры оценки методов авторами исследования [2] была предложена стеганографическая стоимость. Данная характеристика выражает степень изменения носителя информации. Изменением может являться потеря определенной функциональности или ухудшение качества передаваемой информации протоколом после воздействия на него стеганографического метода.

Метод, основанный на модуляции числа фрагментов, имеет довольно низкую стоимость, поскольку его применение не затрагивает поля, нарушающие функционал пакета и его достаточно просто реализовать. Однако метод вносит неравномерности в количество фрагментов в пакете. В свою очередь, метод изменения фрагментов, основанный на *IS* влияет на скорость передачи данных носителем, поскольку применение метода увеличивает общее количество фрагментов пакета. Данный метод можно считать менее обнаруживаемым по сравнению с методов модуляции числа фрагментов. Уже упомянутое комбинирование этих методов уменьшает общую стоимость стеганографии по сравнению со стоимостью методов по отдельности. Такой эффект называется суперпозицией стеганографии.

На основе принципа работы метода *LACK* можно сделать вывод, что метод имеет довольно высокую стоимость, выражающуюся в чувствительности к потере пакетов из-за использования некоторых пакетов для передачи стеганограммы.

Злоупотребление такими потерями может привести к снижению качества передаваемой информации для пользователей. Например, потеря пакетов должна быть не выше 0,3% от общего числа пакетов, чтобы свести к минимуму стоимость и избежать возможности обнаружения.

Сравнительный анализ описанных методов представлен в табл. 1.

Таблица 1.

Метод	**Достоинства**	**Недостатки**	**Особенности**
Изменения фрагментов	1. Сложность стеганоанализа за счет неизменности общего числа фрагментов и их внешнего вида. 2. Дополнительная защита стеганограммы хэш-функцией с заранее известным *Steg*-ключом. 3. Простота реализации.	1. Различие хэш-значения от полученного от исходных данных без вложения. 2. Геометрическое распространение ошибок в результате изменения содержимого пакета.	Обеспечивает практическую неизменность общего вида сетевого трафика, за исключением состава пакета и его хэша, что можно обнаружить методом целенаправленного получения хэш-значения для исходных данных без вложения.

Метод	Достоинства	Недостатки	Особенности
Модуляции числа фрагментов	1. Низкая «стоимость» реализации. 2. Не затрагивает структуру и вид отдельного пакета.	1. Ограниченный объем вложенной информации. 2. Легкость обнаружения. 3. Сложность реализации.	Основан на изменении структуры передачи пакетов, в результате чего число пакетов зависит от передаваемой стеганограммы, что приводит к видоизменению трафика и повышает обнаруживаемость.
Lost Audio Packets (LACK)	1.Возможность передачи стеганограммы за счет временных характеристик, при помощи задержки пакетов. 2.Снижения уровня обнаруживаемся за счет использования комбинированного подхода.	1. Высокая «стоимость» реализации. 2. Низкий процент содержания измененных (стеганографичеких пакетов) за счет чувствительности к потерям пакетов. 3. Реализация зависит от операционной системы.	Гибридный метод, основанный на особенностях видоизменения трафика двух предыдущих и применяемый непосредственно в объемных пакетах телефонии.

Таким образом, объединение нескольких стеганографических методов на одном носителе может снизить общую стоимость стеганографии, что положительно влияет на успешность передачи скрытой информации и уменьшение вероятности ее обнаружения. Также авторы [2] отмечают, что на объединение методов могут потребоваться вычислительные, ресурсные и временные затраты. Однако объединение без каких-либо дополнительных затрат является частным случаем суперпозиционной стеганографии и называется стеганографией с нулевыми затратами.

Сетевые протоколы

Для работы со стеганографией можно применять любые популярные сетевые протоколы, которые будут выступать в роли носителя стеганограммы. Для вставки стеганограммы существуют особые условия изменения полей пакета сетевых протоколов. Поскольку данные поля являются необязательными, то их изменение не окажет влияние на качество передачи данных, однако эти поля можно использовать для скрытой передачи информации, чем успешно пользуются злоумышленники, передавая стеганограммы в компьютерных сетях. В работах [5] и [6] приводится исследование множества различных популярных протоколов, таких как *TCP, UDP, IP*. В работах описываются поля, которые можно применять для сетевой стеганографии.

Протокол *Transmission Control Protocol* (*TCP*) используется для надежной передачи данных между устройствами, который гарантирует доставку пакетов данных между клиентом и сервером в правильной последовательности без потерь. Главными полями, данные в которых могут быть заменены на стеганограмму в этом протоколе являются: поле указатель важности (*Urgent pointer*), поле опции (*Option*), поле порядковый номер (*Sequence Number*), поле контрольная сумма (*Checksum*).

Протокол *User Datagram Protocol* (*UDP*) является протоколом транспортного уровня и используется при передачи большого объема данных в сети, не гарантируя при этом доставку клиентом или подтверждение получения пакетов со стороны сервера. Он является быстрее протокола *TCP* и необходим в средах, где небольшие задержки не сильно критичны. Поля, которые могут заменить свою полезную нагрузку в этом протоколе выступают: поле порт отправителя (*Source port number*), поле *Checksum.*

Интернет-протокол версии 4 (*IPv*6) – это протокол сетевого уровня, который используется для маршрутизации и доставки пакетов с полезной нагрузкой в сети Интернет. Принцип работы протокола основан на определении уникальных *IP*-адресов для каждого устройства в сети Интернет и формировании пакетов для передачи. Полями, которые можно использовать для передачи стеганограммы являются: поле указатель перегрузки (*Explicit Congestion Notification*), поле идентификатор (*Identification*), поле смещение фрагмента (*fragment offset*), поле Option и поле точка дифференцированных услуг (*Differentiated Services Code Point*).

Интернет-протокол версии 6 (*IPv*6) – это усовершенствованная версия протокола *IPv*4, разработанная специально для его замены, так как последний имеет ограниченное количество адресов для выдачи всем системам в сети. *IPv*6 предполагает широкий диапазон адресов. Поскольку данный протокол имеет улучшенную безопасность, то единственным полем для вложения скрытой информации выступает поле метка потока (*Flow label*).

В работах [4] и [7] описываются принципы построения сетевой стеганографии, основанные на использовании *VoIP,* и рассматривается применение протокола *RTP* для использования скрытой передачи данных.

RTP – это протокол, используемый в аудио и видео потоках для доставки данных, в роли которых выступают пакеты в реальном времени через сеть. Данный протокол имеет способы обеспечения механизма синхронизации и управления трафиком. Полями, используемыми для техник стеганографии, являются: поле заполнение (*Padding data*), поле *Sequence number*, поле метка времени (*Timestamp*) и поле *SSRC*-идентификатор.

Существует множество программ, используемых для изменения заголовков и полезной нагрузки сетевых пакетов, а также позволяющих редактировать необязательные поля протоколов, используемые для передачи стеганограммы.

Например, программа *hping* [8] является наиболее популярной бесплатной программой для создания и изменения пакетов. С помощью программы можно формировать и отправлять собственно сформированные *TCP, UDP, ICMP* и *IP* пакеты непосредственно для применения в целях сетевой стеганографии. Данный инструмент предназначен для специалистов, так как не имеет графического интерфейса, однако является кроссплатформенным и поддерживает большое количество операционных систем, например, *Windows, MacOS, Linux, FreeBSD* и т.д.

Программа *Ostinato* [9] имеет открытый исходный код и позволяет работать с сетевыми пакетами. Данная программа также, как и *hping* поддерживает большинство популярных сетевых протоколов, позволяет генерировать сетевые пакеты и является кроссплатформенной. Программа имеет простой графический интерфейс.

Программа *Colasoft Packet Builder* [10] позволяет создавать пользовательские сетевые пакеты, умеет редактировать исходные данные в полях пакетах в формате *HEX* и декодировать их, что позволяет пользователям просто обрабатывать информацию в пакетах. Программа имеет графический интерфейс, в который входят обширные функции для работы с сетевыми данными.

Сравнение особенностей рассмотренных сетевых протоколов в рамках сокрытия информации представлено в табл. 2.

Таблица 2.

Протокол	**Уровень модели *OSI* (*TCP/IP*)**	**Особенности вложения**	**Поля пакета для вложения**	**ПО реализации**
TCP	Транспортный	Принцип гарантированной доставки без потери пакетов усложняет маневры с количеством пакета для вложения.	*Urgent pointer, Option, Sequence Number, Checksum*	*Ostinato*
UDP	Транспортный	Принцип быстрой доставки пакетов с возможными потерями позволяет маневры с их количеством и содержанием, однако понижает степень устойчивости стеганограммы и способен привести к распространению ошибок в геометрической прогрессии, тем самым увеличив вероятность раскрытия.	*Source port number, Checksum*	*Ostinato*
IPv4	Сетевой (межсетевого взаимодействия)	Определяет сетевой адрес отправителя и получателя, видоизменение которого недопустимо и легко обнаруживаемо даже в рамках локальной сети (10.0.0.0/8; 172.16.0.0/16; 192.168.0.0/24).	*Explicit Congestion Notification, Identification, Fragment offset, Option, Differentiated Services Code Point*	*Ostinato Colasoft Packet Builder*
IPv6	Сетевой (межсетевого взаимодействия)	Определяет сетевой адрес отправителя и получателя, однако в силу широкого пула адресов, допускает их изменение при условии использования динамической маршрутизации и *DHCP* сервера.	*Flow label*	*Ostinato Colasoft Packet Builder*

Протокол	**Уровень модели *OSI* (*TCP/IP*)**	**Особенности вложения**	**Поля пакета для вложения**	**ПО реализации**
RTP	Прикладной (приложений)	Имеет возможность размещения стеганоконтейнеров большого объема в силу работы с *VoIP*, однако имеет ограничения в манипуляциях со временем и числом пакетов в силу наличия механизмов обеспечения синхронизации и управления трафиком.	*Padding data, Sequence number, Timestamp, SSRC-идентификатор*	*Ostinato*
ICMP	Сетевой (межсетевого взаимодействия)	Высокая вероятность доставки в связи с тем, что межсетевые экраны и правила зачастую не блокируют данный протокол, удобен при манипуляциях с временными задержками и свободным наполнением поля данных.	*Timestamp, MTU, Data*	*Colasoft Packet Builder hping*

Заключение

Сетевая стеганография – это один из способов, предоставляющий злоумышленникам скрытый обмен информации через легитимные каналы трафика. Такой скрытый обмен информацией позволяет совершать атаки на конфиденциальные системы, закрепляясь в инфраструктуре организации и усложняя процесс выявления и обнаружения аномалий. В данной работе были рассмотрены основные методы скрытой передачи стеганограммы, способы формирования сетевых пакетов, а также инструменты, позволяющие редактировать содержимое пакетов. Понимание основных принципов и технологических методов, с помощью которой осуществляется сетевая стеганография позволяет укрепить меры защиты информации в области сетевого трафика. Поэтому развитие направления обнаружения сетевой стеганографии способствует укреплению уровня защиты сетевых инфраструктур.

Литература

1. Data Obfuscation: Steganography – ATTACK.MITRE. URL: https://attack.mitre.org/techniques/T1001/002/ (дата обращения – февраль 2024).
2. Mazurczyk W, Wendzel S., Ignacio Azagra Villares I, Szczypiorski K On importance of steganographic cost for network steganography //Security and Communication Networks, 2016. – Т. 9. – № 8. – С. 781-790.

3. Пескова О.Ю., Халабурда Г.Ю. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи // Известия Южного федерального университета. Технические науки, 2012. – Т. 137. – № 12 (137). – С. 167-176.
4. Волкогонов В.Н., Гетьман Е.М., Салита А.С. Сокрытие информации в протоколах RTP, RTCP //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021), 2021. – С. 183-188.
5. Забиронин А.Д. Программное средство скрытой передачи информации ограниченного доступа по сетям связи общего пользования, функционирующих на основе стека протоколов TCP/IP. – Пенза, 2018. URL: https://elib.pnzgu.ru/files/eb/doc/6PRXwEekEcBg.pdf (дата обращения – февраль 2024).
6. Волкогонов В.Н., Гетьман Е.М., Салита А.С. Методы и способы создания стеганографических вложений в сетевых пакетах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021), 2021. – С. 178-183.
7. Lehner F., Mazurczyk W., Keller J., Wendzel S. Inter-protocol steganography for real-time services and its detection using traffic coloring approach // 2017 IEEE 42nd Conference on Local Computer Networks (LCN). – IEEE, 2017. – С. 78-85.
8. HPING network tool – Github. URL: https://github.com/antirez/hping (дата обращения – февраль 2024).
9. Packet/Traffic Generator and Analyzer Ostinato – Github. URL: https://github.com/pstavirs/ostinato (дата обращения – февраль 2024).
10. Packet Builder for Network Engineer – Colasoft. URL: https://www.colasoft.com/packet_builder/ (дата обращения – февраль 2024).

ПРИМЕНЕНИЕ СТЕГАНОГРАФИИ ПРИ ОСУЩЕСТВЛЕНИИ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ ПРЕДПРИЯТИЙ

Д.В. Клишин, *Национальный исследовательский университет ИТМО, Danil.Klishin2021@yandex.ru;*
М.Ю. Федосенко, *Национальный исследовательский университет ИТМО, fedosenkomaksim98@gmail.com.*

УДК 004.056

Аннотация. В статье представлено описание тактик компьютерных атак на информационную инфраструктуру предприятий с применением стеганографии. Описаны основные типы стеганографии, а также представлены технологии и процедуры, используемые в реальных компьютерных атаках. В результате исследования выявлены основные тенденции применения стеганографии в компьютерных атаках: алгоритмы вложения и форматы стеганоконтейнеров, вектора атак, используемое программное обеспечение, реальные случаи успешной реализации атак.

Ключевые слова: стеганография; тактики компьютерных атак; техники компьютерных атак; процедуры компьютерных атак; виды стеганографии.

THE USE OF STEGANOGRAPHY IN THE IMPLEMENTATION OF COMPUTER ATTACKS ON THE INFORMATION INFRASTRUCTURE OF ENTERPRISES

D. Klishin, *National Research University ITMO;*
M. Fedosenko, *National Research University ITMO.*

Annotation. The paper describes the tactics of computer attacks on the information infrastructure of enterprises using steganography methods. The main methods of steganography are described, as well as technologies and procedures used in real computer attacks. The study revealed the main trends in the use of steganography in computer attacks: nesting algorithms and formats of steganocontainers, attack vectors, software used, real cases of successful implementation of attacks.

Keywords: steganography; tactics of computer attacks; techniques of computer attacks; procedures of computer attacks; types of steganography.

Введение

В современном мире постиндустриального общества, развитие которого сопровождается наличием информационной революции, появляется острая необходимость в защите информации от ее подмены, наличия в ней ложного содержания и использования в корыстных целях. Современные технологии и эволюционное развитие человеческого мозга приводит к тому, что и абсолютно верная (в рамках рассматриваемой информационной системы) информация может быть атакована недоброжелателями, при этом приносить вред как конкретному индивиду, так и обществу в целом. Другими словами, в качественном информационном контенте может быть спрятан другой контент.

Исследованием данного явления занимается такой раздел науки как Стеганография. Данный раздел изучает способы передачи и/или хранения информации при условии сохранения в тайне самого факта использования такого способа.

Толковый словарь Ушакова дает следующее определение данному термину:

Стенография (от греч. *steganos*-скрытый и *grapho*-пишу) – Тайнопись, письмо условными, шифрованными знаками [1]. Несмотря на схожее определение с понятием криптография, стеганография не занимается шифрованием самого информационного объекта, а определяет методы сокрытия самого факта присутствия этого объекта. Переходя на более простой язык, шифрование при стеганографии заключается в том, что мы встраиваем один информационный объект в другой информационный объект, как вирус встраивается в клетку живого организма, не изменяя внешней структуры самой клетки, в то время как при использовании криптографии сразу будет понятен факт шифрования в виду совсем другой, отличной от обычной, структуры клетки.

Отсюда следуют следующие преимущества стеганографии над криптографией [2]:

- Отсутствие сложных математических моделей (при классической стеганографии) для шифрования информации.
- Отсутствие очевидного факта наличия скрытой информации, при котором злоумышленник даже не подозревает о наличие данной информации, тем самым вероятность обнаружения без специальных знаний и аналитических данных сводится к нулю.
- Возможность использования стеганографии как альтернативы криптографии в условиях, когда использование криптографии невозможно.

В качестве примера к последнему пункту из списка преимуществ можно привести страну Китай, в которой 1 января 2020 г. вступил в силу закон «О Криптографии» [3]. В рамках действия данного законодательного акта,

государственный аппарат будет регулировать криптографические методы и протоколы, использующиеся на территории страны. Конкретнее, будет контролироваться допустимость/недопустимость использования криптографии для каждого конкретного случая, а также сложность криптоключей и наличие возможности дешифровки всех криптографических методов у органов государственной власти. Согласно данному закону, государство не планирует полный отказ от использования криптографии. Наоборот, государство будет поощрять и поддерживать научно-технические исследования в сфере шифрования данных и защищать интеллектуальную собственность на криптографические методы и технологии [4].

Данный пример демонстрирует тенденцию вывода практического применения стеганографии на новый уровень, поскольку потребность в обмене скрытыми данными может возникнуть не только среди нарушителей, но и среди обычных пользователей, не желающих мониторинга своей информации [5]. Но поскольку именно «нежелательные» данные нарушителей, а именно, несвоевременная реакция на них, способны нанести большой ущерб и понести огромные убытки, то необходимо исследовать возможность применения стеганографии в реализации компьютерных атак.

В связи с этим, целью данной статьи является выявление тактик и векторов компьютерных атак на информационную инфраструктуру предприятий с использованием стеганографии на основе информации о реальных случаях реализации подобного рода атак. Для выполнения поставленной цели требуется решить следующие задачи:

- Выявить основные типы и особенности стеганографических контейнеров в зависимости от формата покрывающего объекта.
- Проанализировать реальные случаи осуществления компьютерных атак с использованием стеганографии, выделить особенности реализации.
- Установить результаты практического применения стеганографии в компьютерных атаках для определения особенностей мер защиты от них.
- Выявить основные техники компьютерных атак с использованием стеганографии и сопоставить их с тактиками компьютерных атак.

Методы стеганографии

В изученных источниках информации [6-8] можно выделить шесть основных типов контейнеров, используемых в стеганографии:

- в тексте;
- в изображении;
- в аудио;
- в видео;
- в метаданных;
- в сетевых протоколах.

В случае с текстовым стеганографическим контейнером, стеганография скрывает секретное сообщение внутри фрагмента текста. Простая версия текстовой стеганографии использует первую букву в каждом предложении для формирования скрытого сообщения.

При использовании в качестве контейнера изображения стеганография кодирует секретную информацию, изменяя биты в цветовой гамме. При этом простым примером стеганографии в изображении является использование младших разрядов каждого пикселя изображения.

Для стеганографического контейнера в аудио может использоваться метод изменения младших разрядов каждого байта в аудиофайле, аналогично стеганографии изображений.

При использовании стеганографического контейнера в видео секретное сообщение может быть как в каждом видеокадре, так и в аудиодорожке.

Также возможно сокрытие информации в полях метаданных различных файлов.

Помимо вышеперечисленных методов сокрытия информации возможно использование в качестве стеганографического контейнера сетевого трафика различных сетевых протоколов. Например, данные могут быть скрыты в заголовках *TCP/IP* или полезной нагрузке сетевых пакетов или в *DNS*-запросах, также отправитель может скрыть информацию за счет времени между отправкой различных пакетов.

Основная сложность обнаружения использования стеганографии заключается в установлении факта передачи секретного сообщения, что в совокупности с разнообразными типами стеганографических контейнеров предоставляет злоумышленнику инструмент для компьютерных атак.

Тактики компьютерных атак с использованием стеганографии

Стеганография рассматривается в нормативно-правовых актах РФ в области информационной безопасности от ФСТЭК России [6, 7]. В документе [6] приведена классификация методов стеганографической передачи информации, а также дана сравнительная характеристика стеганографических методов преобразования информации. В документе [7] стеганография упоминается в перечне основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации.

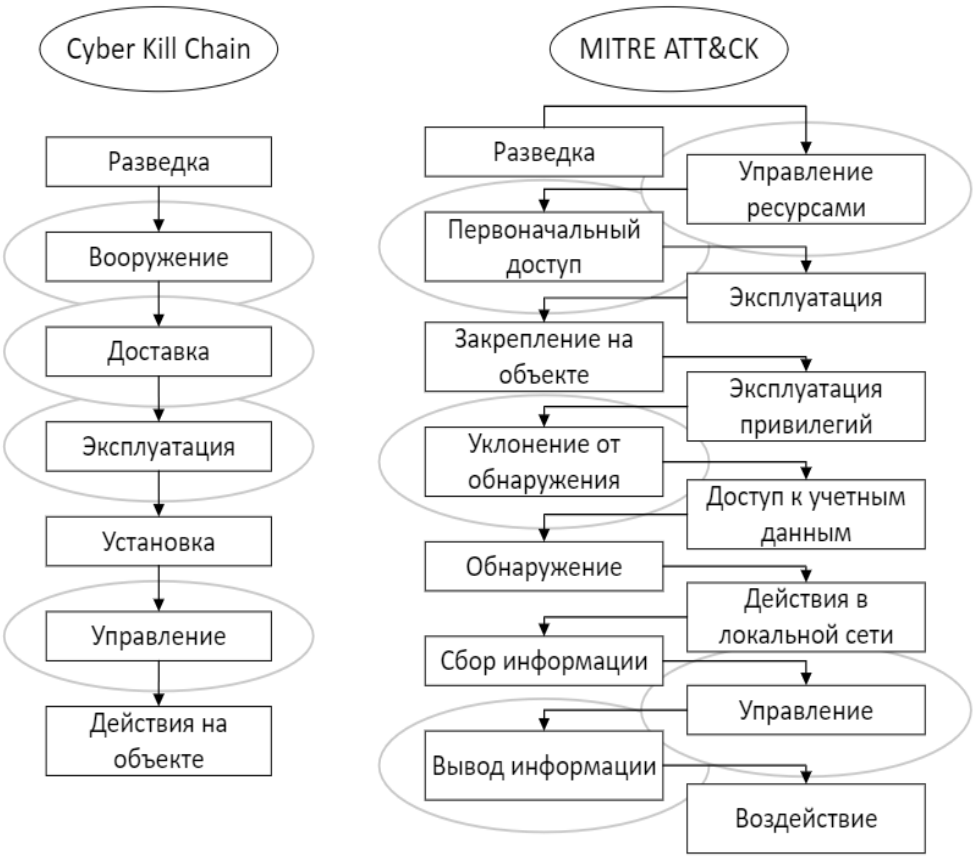

Рисунок 1

Тактики компьютерных атак, в которых используются техники стеганографии можно продемонстрировать на фреймворках *Cyber Kill Chain* [9] и *MITRE ATT&CK* [10]. При анализе базы знаний *MITRE ATT&CK* было выявлено рассмотрение техник стеганографии в таких тактиках компьютерных атак, как управление вредоносным программным обеспечением и в тактике избежания обнаружения. При этом в методике ФСТЭК России [7] также рассматривается применение стеганографии в тактике вывода информации из целевой информационной инфраструктуры. Данное отличие объясняется тем, что для других тактик, например, таких как разработка вредоносного программного обеспечения, получение доступа и вывод данных, процедуры стеганографии идентичны процедурам, описанным в тактике избегания обнаружения. На рис. 1 выделены основные тактики компьютерных атак, в которых может применяться стеганография.

Использование стеганографии в реальных компьютерных атаках

Основной из тактик компьютерных атак, в которой может использоваться стеганография, является предотвращение обнаружения информации, которая доставляется или выводится с целевого объекта в информационной инфраструктуре.

По версии *MITRE* первым вредоносным программным обеспечением, в котором зафиксировано применение стеганографии, является *Duqu*. Вредоносное программное обеспечение *Duqu* было впервые обнаружено в 2011 г., оно использовало стеганографию для скрытного вывода собранной информации из целевой информационной инфраструктуры в изображениях [11].

На данный момент существует большое количество вредоносного программного обеспечения, используемого для скрытой доставки или вывода информации. В табл. 1 перечислено вредоносное программное обеспечение, хакерские группировки, а также каким образом использовалась стеганография в атаках по версии [10, 12].

Таблица 1.

Наименование	**Описание использования стеганографии**
Вредоносное программное обеспечение	
ABK	Может извлечь вредоносный переносимый исполняемый файл из фотографии.
Diavol	Запутывает свои основные процедуры кода в растровых изображениях.
ProLock	Может использовать файлы *JPG* и *BMP* для хранения своей полезной нагрузки.
ObliqueRAT	Может скрывать свою полезную нагрузку в изображениях *BMP*, размещенных на скомпрометированных веб-сайтах.
Raindrop	Использует стеганографию, чтобы определить начало своей закодированной полезной нагрузки в пределах легитимной *zip* кодировки.
PolyglotDuke	Может использовать стеганографию, чтобы скрыть передаваемую информацию в изображениях.
LiteDuke	Использует файлы изображений, чтобы скрыть свой компонент загрузки.
RegDuke	Может скрывать данные в изображениях, включая использование младших разрядов.
RDAT	Может встраивать данные в *BMP* изображение перед выводом.

Наименование	Описание использования стеганографии
IcedID	Имеет встроенные двоичные файлы в зашифрованных *RC*4 файлах *PNG*.
Avenger	Может извлекать вредоносные программы-бэкдоры из загруженных изображений.
build_downer	Может извлекать вредоносное ПО из загруженного файла *JPEG*.
BBK	Может извлечь вредоносный исполняемый файл из фотографии.
Ramsay	Извлекает вредоносный исполняемый файл, встроенный в файлы JPEG, содержащиеся в документах *Word*.
Okrum	Полезная нагрузка зашифрована и встроена в *PNG*-файл.
Bandook	Использует изображения в формате *PNG* в *zip*-файле для создания исполняемого файла.
Invoke-PSImage	Может использовать скрипт *PowerShell* в пикселях файла *PNG*.
PowerDuke	Использует стеганографию для скрытия бэкдоров в *PNG*-файлах, которые также шифруются с использованием алгоритма шифрования *Tiny*.
Хакерские группировки	
Earth Lusca	Использует стеганографию, чтобы скрыть шелл-код в файле изображения *BMP*.
Andariel	Скрывает вредоносные исполняемые файлы в файлах *PNG*.
*TA*551	Скрывает закодированные данные для библиотек *DLL* вредоносных программ в формате *PNG*.
Tropic Trooper	Использует файлы *JPG* с зашифрованной полезной нагрузкой.
MuddyWater	Сохранят запутанный код *JavaScript* в файле изображения с именем *temp.jpg*.
*APT*37	Использует стеганографию для отправки изображений пользователям, в которые встроен шелл-код.
Leviathan	Использует стеганографию, чтобы скрыть украденные данные внутри других файлов, хранящихся на *GitHub*.
BRONZE BUTLER	Использует стеганографию в нескольких операциях, чтобы скрыть вредоносную полезную нагрузку.
Operation Ghost	Во время операции использовалась стеганография, чтобы скрыть полезную нагрузку внутри допустимых изображений.
Компьютерные атаки	
Operation Spalax	Для операции исполнители использовали упаковщики, которые считывают пиксельные данные из изображений, содержащих в себе вредоносные файлы, и создают следующий уровень выполнения на основе этих данных.
ABK	Может извлечь вредоносный переносимый исполняемый файл из фотографии.

Из приведенной выше таблицы можно выделить следующие основные методы использования стеганографии в тактике скрытого ввода и вывода информации:

- Хранение бэкдоров и шелл-кодов.
- Хранение и извлечение компонентов вредоносного программного обеспечения из контейнеров-изображений.
- Обфускация вредоносного кода.
- Скрытие информации в изображении для последующей передачи на сервер злоумышленника [13].

Помимо этого, злоумышленники могут использовать стеганографию в тактике сокрытия трафика управления между сервером атакующего и атакуемым объектом. Как правило, для этого используется стеганография в сетевом трафике, но также может применяться стеганография в изображении. В табл. 2 перечислено вредоносное программное обеспечение, хакерские группировки, а также каким образом использовалась стеганография в атаках по версии [9].

Таблица 2.

Наименование	**Описание использования стеганографии**
Вредоносное программное обеспечение	
Zox	Использует формат файла *PNG* для обмена данными с сервером атакующего.
Sliver	Может кодировать двоичные данные в *PNG*-файл для связи с сервером атакующего.
SUNBURST	Данные передаются как легитимный *XML*, связанный со сборками *.NET*, или как поддельный большой двоичный объект *JSON*.
RDAT	Может обрабатывать стеганографические изображения, прикрепленные к сообщениям электронной почты, для отправки и получения команд с сервера атакующего. Также может встраивать дополнительные сообщения в изображения формата *BMP* для связи с оператором *RDAT*.
LightNeuron	Управляется с помощью команд, которые встроены в *PDF*-файлы и *JPG*-файлы с использованием стеганографических методов.
Duqu	Когда команда и управление Duqu работают по протоколу *HTTP* или *HTTPS, Duqu* загружает данные на сервер атакующего, добавляя их в пустой файл *JPG*.
HAMMERTOSS	Управление осуществляется с помощью команд, которые добавляются к файлам изображений.
Хакерские группировки	
Axiom	Использует стеганографию, чтобы скрыть свои сообщения серверу атакующего.
Компьютерные атаки	
Operation Ghost	Во время атаки используется стеганография, чтобы скрыть связь между целевым объектом и сервером атакующего.

В фреймворке [9] для тактики сокрытия трафика управления между сервером атакующего и атакуемым объектом, в основном, перечислено применение стеганографии в медиафайлах, но к данной тактике также можно отнести применение стеганографии при осуществлении внеполосных атак, например, таких как *DNS-tunneling*.

Как правило, на внешних веб-серверах, находящихся в демилитаризованной зоне, разрешен обмен информации на 53 порту для протокола *DNS*. В результате чего, атакующий может использовать данный протокол как для проведения внеполосных атак на веб-приложения, так и для контроля сервера в случае, если он уже захвачен. Для этого атакующий отправляет *DNS*-запросы с веб-сервера на подконтрольный ему *DNS*-сервер и фиксирует пришедшие на него запросы. При этом информация передается в запрашиваемом поддомене, например: *base64({whoami}).evel.attack.com.*

Данную технику применения стеганографии в компьютерных атаках можно считать наиболее распространенной, так как она используется при эксплуатации таких уязвимостей как *SSRF, SQLi, Command injection* и *XSS*, а эксплуатация данных уязвимостей осуществляется часто из-за большого количества уязвимых веб-приложений согласно [14].

Заключение

Согласно изученным при проведении данного исследования источникам, можно сделать вывод, что в среде разработчиков вредоносного программного обеспечения наблюдается тенденция использования методов стеганографии не только для вывода информации из информационной инфраструктуры предприятий и сокрытия коммуникации с командным центром, но и для доставки модулей вредоносного программного обеспечения на целевой объект [15]. Иными словами, основные подходы, используемые злоумышленниками, заключаются в обфускации (сокрытии) вредоносных компонентов и их последующей доставки на атакуемую систему в «обход» средств защиты информации (СЗИ).

В настоящий момент уже имеются случаи успешной реализации атак с применением стеганографии, в связи с чем в сообществе специалистов компьютерной безопасности выделяются конкретные атаки, реализующие их группировки, программное обеспечение, тактики и техники, отражающие подходы и вектора атак злоумышленников (табл. 2).

В связи с этим, развитие стеганографических техник доставки вредоносного программного обеспечения открывает новые векторы для атак с использованием социальной инженерии, упрощая при этом процесс манипуляции атакуемым работником. Таким образом, организация со зрелым уровнем информационной безопасности должна реализовывать комплексные меры по обеспечению информационной безопасности, как на программно-аппаратном, так и на организационном уровнях. В том числе организация должна осуществлять постоянное тестирование и обучение работников правилам информационной безопасности, а для работников отделов информационной безопасности и информационных технологий должны проводиться периодические киберучения на предмет противостояния новым угрозам.

Литература

1. Ушаков Д.Н. Толковый словарь русского языка // Под ред. Д.Н. Ушакова. Д.Н. М.: Гос. ин-т «Сов. энцикл.»; ОГИЗ; Гос. изд-во иностр. и нац. слов., 1935-1940. (4 т.). – С. 88405.
2. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие // Интермедиа. – Санкт-Петербург, 2017. – С. 312.
3. В Китае принят закон о криптографии. URL: http://d-russia.ru/v-kitae-prinyat-zakon-o-kriptografii.html. (Дата обращения - февраль2024).
4. Encryption Law of the People's Republic of China (Adopted at the 14th meeting of the Standing Committee of the 13th National People's Congress on October 26, 2019) URL: http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml%20 (Дата обращения – февраль 2024).
5. Федосенко М.Ю. Социологическое исследование осведомленности выпускников образовательных учреждений в возможностях скрытого обмена данными в интернете // Скиф. Вопросы студенческой науки, 2022. – № 1 (65). – С. 287-295.
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: – URL: https://fstec.ru/en/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/bazovaya-model-ot-15-fevralya-2008-g (дата обращения – февраль 2024).
7. Методика оценки угроз безопасности информации: – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения – февраль 2024).

8. Федосенко М.Ю., Беззатеев С.В. Анализ проблематики применения методов стеганографии при осуществлении противоправных действий и ее роли в цифровой криминалистике // Проблемы информационной безопасности. Компьютерные системы, 2023. – № 3 (56). – С. 33-57.
9. Cyber Kill Chain: – URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения – февраль 2024).
10. MITRE ATT&CK Enterprise: – URL: https://attack.mitre.org/tactics/enterprise/ (дата обращения – февраль 2024).
11. Целевые атаки типа Duqu 2.0 – URL: https://www.kaspersky.ru/resource-center/threats/duqu-2?ysclid=lsek9g30qx963283925 (дата обращения – февраль 2024).
12. Ахрамеева К.А., Федосенко М.Ю. Сравнительный анализ возможностей использования стеганографического программного обеспечения для скрытого обмена данными в сети интернет // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2022. – № 1. – С. 37-43.
13. Федосенко М.Ю., Бочаров М.В. Анализ используемых алгоритмов сокрытия информации в современном стеганографическом программном обеспечении // Студенческий научно-образовательный журнал «StudNet», 2022. – Т. 5. – № 2. – С. 29.
14. OWASP Top 10 Web Application Security Risks: – URL: https://owasp.org/www-project-top-ten/ (дата обращения – февраль 2024).
15. Никулина Т.В. Выявление вредоносного кода в графических файлах, внедренного с помощью методов стеганографии // Матрица научного познания, 2021. – № 1-2. – С. 62-67.