

НОМЕР 116  
МАРТ, 2025



**ИННОВАЦИИ.**

**НАУКА.**

**ОБРАЗОВАНИЕ**

**ЭЛЕКТРОННОЕ ПЕРИОДИЧЕСКОЕ ИЗДАНИЕ**



УДК 004.02:004.5:004.9

ББК 73+65.9+60.5

Э40

**Э40** Научный электронный журнал «Инновации. Наука. Образование \ Отв. ред. Сафронов А.И. – Тольятти: – 2025.– № 116 (март).– 141 с.– URL: <http://innovjourn.ru>

Журнал публикует научные обзоры, статьи проблемного и научно-практического характера по техническим, педагогическим, химическим, экономическим, физико-математическим, социологическим, историческим, психологическим, философским, филологическим, юридическим наукам и архитектуре.

Все статьи журнала рецензируются.

Журнал индексируется в российских и международных базах цитирования: Elibrary, Research Bible, Google Scholar, Scientific Indexing Services и Polska bibliografia naukowa.

Договор с Elibrary: №185-03/2015 от 26.03.2015 г.

ISSN 2687-1068.

УДК 004.02:004.5:004.9

ББК 73+65.9+60.5

© Научный журнал «Инновации. Наука. Образование», 2015-2025



## Содержание

### Технические науки

<b>Масликов Т.О.</b> .....	
Kali Pi — миниатюрное сверхпортативное устройство для тестирования на проникновение .....	6
<b>Масликов Т.О.</b> .....	
Обзор уязвимостей человека в кибербезопасности: проблемы и решения для микрофинансовых организаций .....	20
<b>Масликов Т.О.</b> .....	
Проблемы кибербезопасности и технологическая интеграция в цепочке поставок военного назначения 4.0.....	31
<b>Земцов Д.С.</b> .....	
Пересечение концепции конфиденциальности по замыслу и поведенческой экономики: подталкивание пользователей к выбору, благоприятному для конфиденциальности.....	44
<b>Александров К.И.</b> .....	
AssessITS : Интеграция процедурных рекомендаций и практических показателей оценки для оценки организационных ИТ-рисков и рисков кибербезопасности .....	51

### Юридические науки

<b>Firiyi Emmanuela Esaie Boukar</b> .....	
Digital law: navigating the legal landscape of the digital age .....	69
<b>Firiyi Emmanuela Esaie Boukar</b> .....	
The role of lawyers in the global financial market .....	72
<b>Зинин Н.В.</b> .....	
Законная неустойка: теоретические и практические аспекты.....	75
<b>Сокоп А.А.</b> .....	
Наследование по закону и завещанию: теория и практика .....	79

### Экономические науки

<b>Ишимов Д.В.</b> .....	
Эффективные методы создания автоворонок в digital-маркетинге .....	89
<b>Пиликина Е.А., Кулакова Ю. В.</b> .....	
Изменение ключевой процентной ставки, ее влияние на кредиты, ипотеку и вклады за вторую половину 2024 года .....	99

### Исторические науки

<b>Чжэн Гуанцзе, Дай жуй</b> .....	
Детская литература периода Великой Отечественной войны: героизм и трогательная беззащитность юных защитников Родины .....	116



**Педагогические науки**

<b>Скляренок И.В., Степанова Н.В., Филиппова Н.В.</b> .....	
Методическая разработка по дополнительному образованию в ДОУ как ступень для развития детей старшей группы по художественно-эстетическому развитию на тему: «Краски осени» .....	118
<b>Алексеева Л.И.</b> .....	
Стратегия подготовки к выпускным экзаменам ОГЭ и ЕГЭ по английскому языку.....	122
<b>Ташлык В.А.</b> .....	
Формирование исследовательских умений младших школьников через проектную деятельность на уроках естествознания .....	127
<b>Постивая Н.Н., Спивак И.А.</b> .....	
Исторические аспекты активности молодежи в рамках хореографического коллектива ....	132
<b>Гусейнов В.Ф.</b> .....	
Проблемы патриотического воспитания в условиях глобальной цифровизации .....	139



## Технические науки



Масликов Тимофей Олегович

Студент 5 курс, факультет КБ

Институт телекоммуникаций им. проф. М.А. Бонч-Бруевича

## КАЛИ PI — МИНИАТЮРНОЕ СВЕРХПОРТАТИВНОЕ УСТРОЙСТВО ДЛЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Аннотация: Тестирование на проникновение играет важную роль в обеспечении безопасности во все более взаимосвязанном мире. Несмотря на достижения в области технологий, ведущие к появлению более компактных и портативных устройств, тестирование на проникновение по-прежнему зависит от традиционных ноутбуков и компьютеров, которые, хотя и портативны, не обладают настоящей сверхпортативностью. В этой статье рассматривается потенциальное влияние разработки специализированного сверхпортативного недорогого устройства для тестирования на проникновение на ходу. Такое устройство могло бы воспроизводить основные функции современных инструментов тестирования на проникновение, включая те, что есть в Kali Linux, в компактном форм-факторе, который легко помещается в кармане. Предлагая удобство и портативность, схожие со смартфоном, это инновационное устройство может переопределить способ работы тестировщиков на проникновение, позволяя им носить с собой необходимые инструменты, куда бы они ни пошли, и гарантируя, что они всегда готовы эффективно проводить оценку безопасности. Этот подход направлен на то, чтобы произвести революцию в тестировании на проникновение, объединив высокую функциональность с непревзойденной портативностью.

*Ключевые слова:* Тестирование на проникновение, Портативное устройство, Кибербезопасность, Raspberry Pi, Информационная безопасность, СПбГУТ им. Проф. Бонч-Бруевича.

*Keywords:* Penetration Testing, Portable Device, Cybersecurity, Raspberry Pi, Information security, SPbSUT im. Prof. Bonch-Bruevich.

Компания Offensive Security разработала адаптированную версию Kali Linux для Raspberry Pi, оптимизированную для работы на устройствах с объемом оперативной памяти не менее 512 МБ и процессором с частотой 900 МГц. Однако для тестирования на



проникновение часто требуется значительная вычислительная мощность, особенно для ресурсоемких задач, таких как атаки по словарю или методом подбора. Ограниченный процессор и оперативная память на Raspberry Pi могут привести к снижению производительности или даже сделать некоторые задачи невыполнимыми. Чтобы преодолеть эти ограничения, можно связать две системы Raspberry Pi, что фактически удвоит доступную вычислительную мощность. Такая конфигурация повышает способность устройства справляться с более сложными задачами, обеспечивая более плавную производительность для сложных мероприятий по тестированию на проникновение. Одноплатные компьютеры (SBC) часто рассматриваются как современное изобретение, но первый SBC, «dyna micro» (позже MMD-1), был представлен в 1976 году компанией E&L Instruments. Основанный на архитектуре Intel, он интегрировал ввод-вывод, дисплей, память и пользовательский ввод на одной плате. SBC столкнулись с проблемами в конце 20-го века из-за ограниченной миниатюризации и высокой стоимости, поскольку персональные компьютеры больше фокусировались на материнских платах, подключенных к дочерним платам для функций ввода-вывода.

1960-е годы ознаменовали начало компьютерной безопасности, поскольку доступ к сети расширился, представляя новые угрозы. В 1967 году был придуман термин «проникновение» для описания системных атак, подчеркивая необходимость тестирования на проникновение для выявления уязвимостей и повышения безопасности. Джеймс П. Андерсон, ведущий эксперт в этой области, выделил шесть ключевых этапов атаки:

- Выявление уязвимостей
- Разработка атаки
- Тестирование атаки
- Захват линии связи
- Выполнение атаки
- Использование входа

Эти ранние разработки заложили основу современных методов тестирования на проникновение.

Спрос на одноплатные компьютеры (SBC) вырос благодаря усилиям таких компаний, как Raspberry Pi, BeagleBoard.org и Arduino в 2000-х годах, которые разработали доступные и удобные для пользователя микроконтроллеры. Это привело к



более широкому внедрению и снижению цен на SBC и системы на кристалле (SoC). Выпуск в 2011 году Raspberry Pi за 35 долларов, разработанный командой Кембриджского университета для студентов, изучающих программирование, произвел революцию в вычислительной технике и приобрел всемирную популярность. Тестирование на проникновение развивалось от ранних инструментов, таких как Multics в 1960-х годах, до SATAN 1990-х годов, который проложил путь для Nmap и Nessus. В 2006 году Offensive Security выпустила BackTrack, который в 2013 году превратился в Kali Linux. Теперь Kali Linux является ведущей ОС для тестирования на проникновение, предлагая такие инструменты, как Nmap, Wireshark и Metasploit. Сочетание Raspberry Pi с Kali Linux обеспечивает портативное, высокопроизводительное решение для тестировщиков на проникновение, сокращая разрыв между портативностью и возможностями, а также делая передовые инструменты более доступными. «Многие из современных одноплатных компьютеров стали настолько мощными, что начинают конкурировать с современными ПК и планшетами». — Клифф Ортмейер, глобальный руководитель отдела разработки решений.

Это утверждение отражает растущую вычислительную мощность одноплатных компьютеров (SBC) в современных технологиях. Появление Raspberry Pi ознаменовало собой значительный сдвиг, уменьшив вычислительную технику до размера кредитной карты без ущерба для функциональности. С выпуском Raspberry Pi 3 в 2016 году SBC начали предлагать производительность на уровне персональных компьютеров, оснащаясь четырехъядерным процессором ARM Cortex-A53, 1 ГБ оперативной памяти и улучшенными возможностями ввода-вывода. Используя SD-карту в качестве загрузочного устройства хранения данных и установив Kali Linux, Raspberry Pi можно превратить в компактную портативную платформу для тестирования на проникновение или цифровой криминалистики. Raspberry Pi — это микрокомпьютер размером с кредитную карту, или одноплатный компьютер (SBC), разработанный педагогами, чтобы предоставить студентам доступную платформу для изучения программирования. Первоначально предложенный в 2006 году и основанный на микроконтроллере Atmel ATmega644, он был выпущен для публики после пяти лет разработки.

Запуск Raspberry Pi вызвал сильный спрос на миниатюрные одноплатные компьютеры и подстегнул конкуренцию. BeagleBone был первым крупным конкурентом, выпустившим свой собственный одноплатный компьютер, за которым последовали другие продукты, такие как R10TBOARD и PANDABOARD ES. Однако Raspberry Pi



быстро стал лидером рынка, продав более двух миллионов единиц за первые два года. Хотя одноплатный компьютер BeagleBone был выпущен в том же году, он не смог сравниться по популярности с Raspberry Pi. Несмотря на схожие характеристики, RIoTBOARD и PANDABOARD ES с трудом набирали обороты, оставив Raspberry Pi и BeagleBoard доминирующими игроками на рынке одноплатных компьютеров.

Основной конкурент Kali Linux, Backbox, был выпущен в 2010 году как альтернатива Kali (ранее BackTrack). Оба они пользуются уважением в сообществе кибербезопасности, но они различаются по возможностям и функциям.

Набор возможностей: Kali Linux выделяется обширной коллекцией из более чем 600 предустановленных инструментов по сравнению с чуть более чем 70 инструментами в Backbox. Этот обширный набор инструментов дает Kali Linux значительное преимущество, поскольку он охватывает широкий спектр задач, таких как тестирование на проникновение, цифровая криминалистика, сетевой анализ и оценка уязвимости. Этот всеобъемлющий набор позволяет специалистам по безопасности решать разнообразные задачи в одной унифицированной среде.

Графический пользовательский интерфейс (GUI): GUI Kali Linux разработан интуитивно понятным и удобным для пользователя, что упрощает навигацию как для новичков, так и для опытных пользователей. Интерфейс оптимизирован для эффективного управления задачами с настраиваемыми параметрами для доступности и оптимизации рабочего процесса. Напротив, GUI Backbox более традиционный и может быть более сложным для новых пользователей, особенно тех, кому требуется более быстрый доступ к инструментам тестирования на проникновение.

Уязвимости: Когда дело доходит до безопасности, Kali Linux обычно считается более безопасным, имея всего 85 задокументированных уязвимостей в базе данных CVE. С другой стороны, Backbox имеет 422 уязвимости, которые могут представлять более высокий риск для пользователей, полагающихся на него для критических задач безопасности. Меньшее количество уязвимостей Kali Linux отражает его постоянные обновления и особое внимание к безопасным методам разработки.

Реагирование на инциденты: Kali Linux отлично справляется с реагированием на инциденты, поскольку оснащен широким набором инструментов, которые облегчают быстрое обнаружение, анализ и смягчение последствий инцидентов безопасности. С такими инструментами, как The Sleuth Kit, Volatility и Autopsy, Kali Linux предоставляет полный набор возможностей для криминалистики и реагирования на инциденты. Для



сравнения, Backbox предлагает меньше специализированных инструментов для реагирования на инциденты, что делает его менее универсальным в обработке событий безопасности в реальном времени или расследований после инцидентов.

Подводя итог, можно сказать, что Kali Linux с его расширенным набором инструментов, улучшенным пользовательским интерфейсом, надежной безопасностью и специализированными возможностями реагирования на инциденты является предпочтительным выбором для тестировщиков на проникновение, экспертов по цифровой криминалистике и специалистов по кибербезопасности. Его постоянное развитие гарантирует, что он остается на передовой безопасности, предоставляя пользователям самые передовые инструменты, доступные в этой области.

Мы живем в цифровую эпоху, когда все — от банковских транзакций до личных фотографий — хранится в сети благодаря многолетним глобальным исследованиям и разработкам. Однако этот прогресс вызывает растущую обеспокоенность по поводу цифровой безопасности. Недавний отчет RAND показывает, что 65 миллионов американцев ежегодно становятся жертвами утечек данных, что приводит к миллиардным убыткам от киберпреступлений. С более чем 6,4 миллиардами долларов, потраченными каждый год на проверки безопасности и тестирование на проникновение, Kali Raspberry Pi предлагает экономически эффективное решение. Используя несколько устройств, организации могут сократить время простоя и повысить эффективность, экономя время и деньги при выполнении ресурсоемких задач.

Устройства Kali Pi — это универсальные инструменты, которые можно использовать для самых разных целей в области кибербезопасности и тестирования на проникновение. Ниже приведены некоторые ключевые применения:

1) Проактивная безопасность: Kali Pi идеально подходит для тестирования на проникновение, позволяя группам безопасности выявлять и устранять уязвимости с помощью таких инструментов, как Wireshark, Nmap, Nessus, Metasploit и John the Ripper для комплексного сканирования и моделирования атак.

2) Реактивная безопасность: при реагировании на инциденты Kali Pi помогает отслеживать следы атак и анализировать нарушения, используя криминалистические инструменты Kali Linux, такие как криминалистика ОЗУ, восстановление паролей и сетевая криминалистика, для выявления угроз и восстановления данных.

3) Безопасность беспроводных сетей: Kali Pi отлично справляется с тестированием безопасности Wi-Fi, используя такие инструменты, как Aircrack-ng, для аудита



уязвимостей сети, взлома паролей и тестирования протоколов шифрования на предмет слабых мест.

4) Мониторинг сети: с помощью таких инструментов, как Wireshark и tcpdump, Kali Pi позволяет анализировать сетевой трафик в режиме реального времени для обнаружения несанкционированной активности и обеспечения работоспособности сети.

5) Анализ вредоносных программ: Kali Pi может анализировать подозрительные файлы и изучать поведение вредоносных программ с помощью таких инструментов, как Cuckoo Sandbox и Volatility, помогая обнаруживать и нейтрализовывать угрозы.

6) Тестирование социальной инженерии: используя такие инструменты, как SET (Social Engineering Toolkit), Kali Pi может имитировать фишинговые и целевые фишинговые атаки для проверки защиты и повышения осведомленности сотрудников.

В целом устройство Kali Pi представляет собой мощный портативный инструмент для тестирования на проникновение, реагирования на инциденты, обеспечения безопасности беспроводных сетей, анализа вредоносных программ и мониторинга сетей, предоставляя экономически эффективное решение для специалистов по кибербезопасности. Устройство Kali Pi, хотя и является мощным инструментом для законного тестирования на проникновение и оценки безопасности, также может быть использовано не по назначению, если попадет в чужие руки. Вот несколько способов, которыми устройство может быть использовано в вредоносных целях:

Несанкционированное тестирование: может использоваться для взлома систем или сетей без разрешения, что может привести к краже данных или сбоям в обслуживании.

Взлом Wi-Fi: такие инструменты, как Aircrack-ng и Wireshark, могут позволить взломать сети Wi-Fi и перехватить данные.

Взлом паролей: такие инструменты, как John the Ripper, можно использовать для взлома паролей и получения несанкционированного доступа.

Использование уязвимостей: Kali Pi может использовать уязвимости системы, используя такие инструменты, как Metasploit, для получения контроля над устройствами.

Социальная инженерия: устройство может использоваться для создания фишинговых сайтов или атак с использованием социальной инженерии с целью кражи учетных данных.

Создание ботнета: может быть частью ботнета для запуска DDoS-атак или других вредоносных действий.



Наблюдение: Kali Pi можно использовать для перехвата пакетов и отслеживания онлайн-активности, что нарушает конфиденциальность.

Распространение вредоносного ПО: вредоносное ПО может распространяться на уязвимые системы через USB-порты или сетевые атаки.

Следуя этим рекомендациям, вы сможете создать высокофункциональное и портативное устройство Kali Pi для эффективного тестирования на проникновение. Это исследование будет использовать методологию наблюдательного исследования для решения исследовательских вопросов. Наблюдения будут проводиться в ходе реализации проекта, и будут сделаны тщательные заметки для обеспечения точных ответов на исследовательские вопросы, изложенные в предложении. 1) Какие следы может оставить Kali Pi в среде тестирования на проникновение?

Footprinting — это метод сбора информации о компьютерной системе и ее сущностях. Каждое устройство в современном вычислительном мире имеет следы, и эти следы можно собрать с помощью различных инструментов компьютерной безопасности, таких как Nmap, ping-сканирование, снятие отпечатков ОС, сканирование TCP/UDP, перечисление сетей и Net Discover.

Чтобы обнаружить следы системы Raspberry Pi, необходимо выполнить следующие семь шагов:

- а) Сбор информации
- б) Определение радиуса действия сети
- в) Определение активных машин
- г) Поиск открытых портов и точек доступа
- е) Идентификация ОС
- ф) Услуги по снятию отпечатков пальцев
- ж) Картографирование сети

Kali Pi функционирует как любая полноценная система пентестинга, оставляя следы в тестовой среде, которые должны тщательно контролироваться. Хорошо спланированная стратегия имеет решающее значение для минимизации или устранения этих следов. Хотя первоначальное сканирование Nmap не смогло обнаружить ОС Kali Pi, Wireshark успешно идентифицировал сетевую активность. Kali Pi разработан как портативная, экономичная альтернатива более крупным и дорогим устройствам, которые сложнее транспортировать и использовать.



2) Каковы шаги по созданию ультрапортативного устройства, способного проводить тестирование на проникновение, как обычный компьютер или ноутбук?

Создание сверхпортативной системы тестирования на проникновение, такой как Kali Pi, требует баланса между размером и мощностью. Ключевые факторы включают:

Вычислительная мощность: мощный процессор и достаточный объем оперативной памяти для выполнения задач по тестированию на проникновение.

Источник питания: внутренняя батарея с длительным сроком службы, обеспечивающая портативность без постоянного источника питания.

Механизм ввода: сенсорный экран или клавиатура с поддержкой Bluetooth для удобного ввода и вывода данных.

Однако создание Kali Pi сопряжено с трудностями. Kali Linux поддерживает Raspberry Pi, но не имеет драйверов дисплея, требуя подключения HDMI, что противоречит переносимости. Кроме того, ОС не поставляется с предустановленными инструментами, требуя ручной установки метапакетов. Для полной функциональности Kali Pi требуется версия Kali Linux с драйверами дисплея и предустановленными инструментами.

3) Каково текущее состояние портативных устройств для пентеста в 2016 году?

В 2016 году ноутбуки были основными портативными устройствами для тестирования на проникновение из-за их мощности и времени автономной работы, но они дороги и не очень портативны. Цель этого проекта — создать устройство, которое в 10 раз меньше, но сохраняет все возможности ноутбука, что произведет революцию в тестировании на проникновение. В случае успеха это сверхпортативное устройство может установить новый стандарт. Хотя инструменты тестирования на проникновение развивались, аппаратное обеспечение в основном осталось прежним. Kali Pi решает эту проблему, уменьшая размер устройства на 80% и веся всего 0,4 фунта, что делает его большим шагом вперед в портативности для тестеров на проникновение.

4) Для каких целей можно использовать устройство Kali Raspberry Pi?

Операционная система Kali Linux, установленная на системе Raspberry Pi, теоретически может быть использована в качестве замены для текущих устройств, которые используются для проведения тестирования на проникновение, таких как ноутбуки и персональные компьютеры, но практическая применимость этой теории еще не проверена. Kali Linux Raspberry Pi будет тестироваться на основе следующих фаз:

а) Отпечаток стопы



- б) Сканирование
- в) Перечисление
- г) Сканирование уязвимостей
- д) Использование уязвимостей
- е) Поддержание доступа

Kali Pi стремится заменить традиционные инструменты тестирования на проникновение, выполняя такие важные задачи, как отпечаток, сканирование и перечисление. Он также будет выполнять сканирование уязвимостей, эксплуатировать слабые места и поддерживать доступ. Kali Pi, доступный по цене и сверхпортативный, доступен для всех уровней навыков и позволяет проводить одновременное тестирование на нескольких устройствах для повышения эффективности, что делает его потенциальным игроком, который изменит правила игры в тестировании на проникновение.

Kali Pi построен на базе Raspberry Pi 3, на котором установлена операционная система Kali Linux 2.0. Kali Pi состоит из различных аппаратных и программных компонентов, и почти все эти компоненты необходимо настроить, что делает это довольно утомительной задачей.

Ниже приведены требования к оборудованию для создания микрокомпьютера:

Raspberry Pi 3 (модель В) (см. рисунок 1 ).

Для разработки Kali Pi необходимо иметь мощный процессор и достаточный объем оперативной памяти, поскольку задачи тестирования на проникновение могут быть весьма ресурсоемкими. Самой мощной версией одноплатного компьютера Raspberry Pi является Raspberry Pi 3 Model B, которая основана на архитектуре ARM.

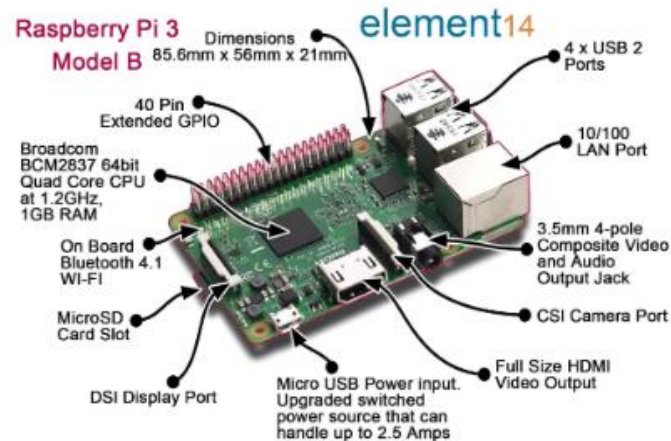


Рисунок 1. Raspberry Pi 3.

Kali Linux можно загрузить с официального сайта, с версией, адаптированной для моделей Raspberry Pi на базе архитектуры ARM. Эта версия предназначена для headless-настроек, и для ее использования с дисплеем требуются дополнительные драйверы.

Установка Kali Linux на Raspberry Pi может быть сложной, но Osoyoo.com упрощает процесс, предлагая версию с предустановленными драйверами дисплея KeDei. Для установки используйте такие инструменты, как Win32DiskImager, чтобы записать образ на карту Micro SD, которая служит хранилищем Raspberry Pi. Базовый образ Kali Linux не включает в себя инструменты тестирования на проникновение. Чтобы получить доступ к полному набору, вам нужно будет загрузить и установить метапакет с веб-сайта Kali Linux. Обнаружение цели: для обнаружения целевой машины отправляется PING на устройство Kali Pi, как показано на рисунке 2.



Рисунок 2. Пинг.

Перечисление хостов: чтобы собрать информацию о целевой машине, проведите сканирование Nmap, направленное на идентификацию операционной системы, как показано на рисунке 3. Это сканирование может раскрыть важные сведения об операционной системе цели, которые могут быть полезны на этапе эксплуатации при тестировании на проникновение.

Командная строка: Nmap-O 192.168.1.26



Рисунок 3. Сканирование ОС.

Сканирование портов: Nmap можно использовать для сканирования портов и определения запущенных на них служб, а также их версий, как показано на рисунке 4. Было проведено сканирование версий служб, в результате чего был получен список открытых портов вместе с соответствующими службами и их версиями.



Командная строка: Nmap-sV 192.168.1.26

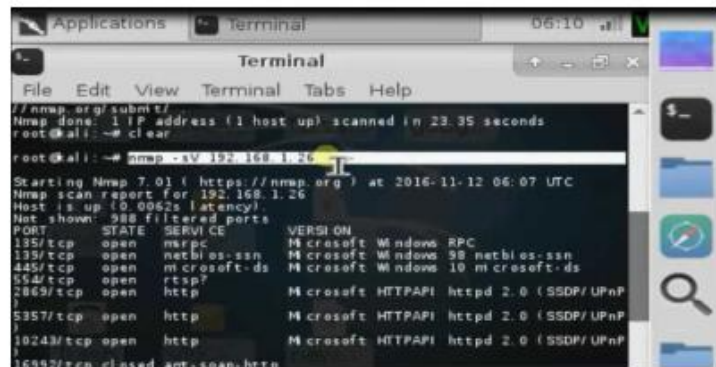


Рисунок 4. Сканирование версии сервиса.

Сканирование уязвимостей: После завершения фазы перечисления хостов следующим логическим шагом было выполнение сканирования уязвимостей, как показано на рисунке 5. Пакет сканера уязвимостей OpenVAS был загружен и установлен на устройстве Kali Pi. Затем OpenVAS использовался для проведения сканирования уязвимостей, в результате чего был сгенерирован список уязвимостей и журналов, которые потенциально могли быть использованы в системе.

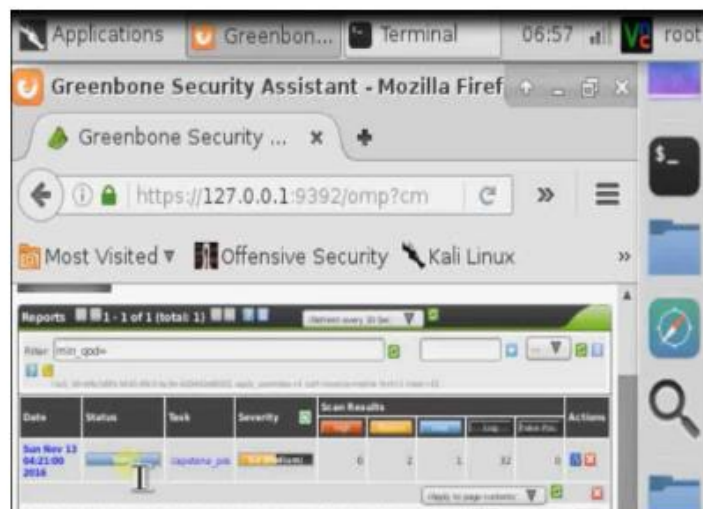


Рисунок 5. Сканирование уязвимостей OpenVas.

Эксплуатация: Kali Pi — это устройство, которое работает как обычная система и может использоваться для всех задач тестирования на проникновение, как показано на



рисунке 6. Такие инструменты, как Metasploit, могут использоваться для эксплуатации уязвимостей целевой системы.

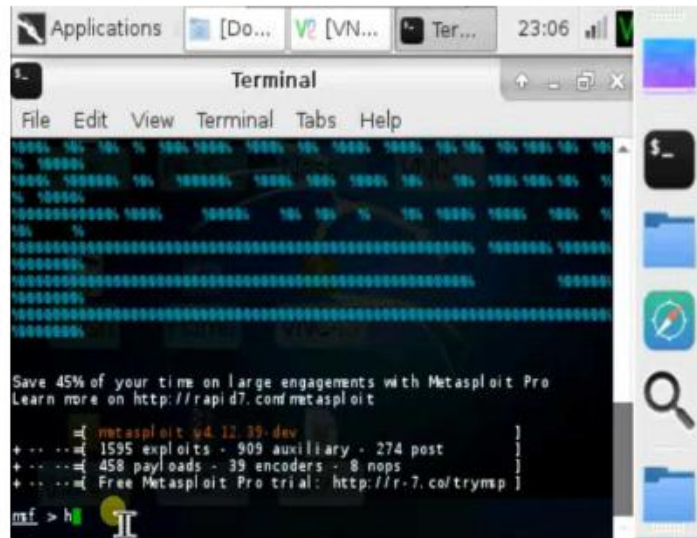


Рисунок 6. Консоль MSF.

Заключение: Индустрия информационной безопасности в первую очередь фокусируется на программном обеспечении и инструментах, при этом значительный акцент делается на разработке ресурсов для тестировщиков на проникновение. Однако аппаратному обеспечению, используемому в этой области, уделяется сравнительно мало внимания. Следовательно, разработка аппаратного обеспечения в значительной степени зависит от компаний, которые производят персональные компьютеры, которые не предназначены специально для тестирования на проникновение. Kali Pi решает эту проблему, предоставляя усовершенствования программного и аппаратного обеспечения, специально разработанные для тестирования на проникновение. Это самое доступное устройство, способное выполнять тесты на проникновение, и предназначенное для студентов и начинающих тестировщиков на проникновение, которые начинают изучать обширный мир информационной безопасности. В сегодняшнем быстро развивающемся технологическом ландшафте информационной безопасности и разведки Kali Pi представляет собой важный шаг в правильном направлении.



**Литература:**

1. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «Умный дом» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 316-321.
2. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270.
3. Гельфанд А. М. и др. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия. – Т. 1. – С. 21-27.
4. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей. – 2018.
5. Шемякин С. Н., Гельфанд А. М., Орлов Г. А. Критическая информационная инфраструктура //Наука и инновации-современные концепции. – 2020. – С. 114-118.



Масликов Тимофей Олегович

Студент 5 курс, факультет КБ

Институт телекоммуникаций им. проф. М.А. Бонч-Бруевича

## ОБЗОР УЯЗВИМОСТЕЙ ЧЕЛОВЕКА В КИБЕРБЕЗОПАСНОСТИ: ПРОБЛЕМЫ И РЕШЕНИЯ ДЛЯ МИКРОФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Аннотация: В этом обзоре рассматриваются уязвимости человека в кибербезопасности в микрофинансовых организациях, анализируется их влияние на организационную устойчивость. Сосредоточившись на социальной инженерии, недостаточном обучении по безопасности и слабых внутренних протоколах, исследование выявляет ключевые уязвимости, усугубляющие киберугрозы для МФО. Обзор литературы с использованием таких баз данных, как IEEE Xplore и Google Scholar, сосредоточен на исследованиях с 2019 по 2023 год, посвященных человеческому фактору в кибербезопасности, характерному для МФО. Анализ 57 исследований показывает, что преобладают фишинг и внутренние угрозы, при этом попытки фишинга ежегодно увеличиваются на 20%. Восприимчивость сотрудников к этим атакам усиливается из-за недостаточного обучения, причем самые высокие показатели уязвимости демонстрируют сотрудники начального уровня. Кроме того, только 35% МФО предлагают регулярное обучение по кибербезопасности, что существенно влияет на сокращение инцидентов. В этом документе рекомендуется повышенная частота обучения, надежный внутренний контроль и культура осведомленности о кибербезопасности для снижения киберрисков, вызванных человеком, в МФО.

*Ключевые слова:* Уязвимости человека , Кибербезопасность , Микрофинансовые организации , Киберугрозы , Осведомленность о кибербезопасности , Снижение рисков, Информационная безопасность, СПбГУТ им. Проф. Бонч-Бруевича.

*Keywords:* Human Vulnerabilities, Cybersecurity, Microfinance Institutions, Cyber Threats, Cybersecurity Awareness, Risk Mitigation, Information security, SPbSUT im. Prof. Bonch-Bruevich.

Микрофинансовые организации (МФО) играют важную роль в продвижении финансовой доступности, особенно в развивающихся странах. Они предлагают



финансовые услуги маргинализированным сообществам, позволяя им получать кредиты, сбережения и страховые возможности. Тем не менее, с ростом использования цифровых технологий МФО для улучшения предоставления услуг, они подвергаются более высокому риску киберугроз.

Среда кибербезопасности для МФО сложна и характеризуется растущей частотой кибератак, использующих человеческие слабости, такие как социальная инженерия и внутренние риски. МФО, наряду с другими частями финансовой индустрии, являются основным объектом внимания киберпреступников из-за конфиденциальной информации, которой они управляют, и потенциальной прибыли от успешных нарушений.

Кибербезопасность МФО характеризуется уникальным набором проблем, которые вытекают из их операционных рамок и социально-экономических контекстов, в которых они работают. Согласно, МФО часто не хватает финансовых ресурсов для инвестирования в передовые меры кибербезопасности, что делает их уязвимыми для атак, таких как утечки данных и финансовое мошенничество.

Кроме того, указывает на то, что ограниченная осведомленность сотрудников о протоколах кибербезопасности усугубляет эти уязвимости, поскольку сотрудники могут не осознавать важность соблюдения правил безопасности. Растущая сложность киберугроз, таких как атаки с использованием социальной инженерии, представляет значительные риски для целостности и конфиденциальности конфиденциальных финансовых данных, хранящихся в МФО. Человеческие уязвимости часто упоминаются как самое слабое звено в структурах кибербезопасности.

Кибербезопасность МФО сопряжена с рядом проблем, включая соблюдение нормативных требований, которые требуют защиты конфиденциальных данных клиентов. Нормативная база, регулирующая кибербезопасность, развивается, и многие правительства и соответствующие органы признают необходимость более надежной защиты от киберугроз. Например, в Кении Центральный банк разработал руководящие принципы для финансовых учреждений по улучшению их кибербезопасности.

Однако соблюдение этих правил может быть сложным для МФО, особенно с ограниченными ресурсами. Отсутствие четких руководящих принципов и поддержки для внедрения мер кибербезопасности может помешать МФО защищать конфиденциальную информацию клиентов и поддерживать соответствие требованиям законодательства. Кроме того, динамичный характер киберугроз требует постоянной бдительности и адаптации, что может быть сложным для учреждений с ограниченными ресурсами.



Культура организации в МФО имеет решающее значение для влияния на то, как сотрудники видят и действуют в отношении кибербезопасности. Подчеркивание безопасности и содействие прозрачным обсуждениям рисков может значительно снизить восприимчивость людей. С другой стороны, культура, которая игнорирует важность кибербезопасности или не предлагает достаточной поддержки обучения, может усугубить слабые стороны и повысить вероятность нарушений безопасности.

Обучение и образование сотрудников являются важнейшими элементами успешной стратегии кибербезопасности. Последовательные обучающие сессии, включая осведомленность о фишинге, управление паролями и защиту данных, могут помочь сотрудникам выявлять и реагировать на потенциальные угрозы. Тем не менее, многочисленные микрофинансовые организации считают сложным выделять достаточные ресурсы на обучающие инициативы, что приводит к дефициту знаний и навыков их сотрудников.

Согласно данным, постоянные инвестиции в обучение и образование имеют решающее значение для развития рабочей силы, способной адаптироваться к изменяющейся среде кибербезопасности. Технологии и системы, используемые МФО, также могут подвергать людей риску. Устаревшее программное обеспечение, недостаточные меры безопасности и пробелы в интеграции систем могут привести к уязвимостям для кибератак.

Кроме того, если сотрудники считают технологию обременительной или неэффективной, они могут быть менее склонны следовать протоколам безопасности. Обновление и создание удобных для пользователя технологий может улучшить соблюдение протоколов безопасности и снизить вероятность человеческих ошибок. Еще одной критической проблемой человеческой уязвимости для МФО является угроза, исходящая от инсайдеров. Согласно, инсайдерские угрозы возникают, когда сотрудники, подрядчики или сторонние сотрудники злоупотребляют своим доступом к конфиденциальной информации, как намеренно, так и непреднамеренно. МФО часто работают в финансовой среде с высокими ставками, что делает их подверженными внутренним рискам безопасности, таким как мошенничество, манипулирование данными или несанкционированный доступ к клиентским счетам.

Это может быть следствием недостаточного внутреннего контроля или неэффективных механизмов мониторинга, которые не способны обнаружить или предотвратить подозрительную деятельность. Кроме того, когда сотрудники не проходят



надлежащую проверку или политики кибербезопасности применяются ненадлежащим образом, инсайдеры становятся серьезным риском для кибербезопасности организации, часто с более разрушительными последствиями, чем внешние атаки.

Отсутствие комплексного обучения кибербезопасности и культуры осведомленности о безопасности среди сотрудников является еще одним серьезным направлением киберугрозы в МФО. Согласно, многие МФО работают в условиях ограниченного бюджета, что может ограничивать инвестиции в адекватные программы обучения кибербезопасности. В результате сотрудники могут не иметь необходимых знаний о безопасных онлайн-практиках, таких как выявление попыток фишинга, защита паролей или понимание политик защиты данных.

Без адекватной подготовки сотрудники плохо подготовлены к распознаванию или предотвращению киберугроз, что значительно увеличивает вероятность нарушений. Создание культуры киберосведомленности также является сложной задачей в МФО, поскольку требует постоянного обучения, регулярных обновлений политики и вовлеченности руководства для внедрения методов обеспечения безопасности в ежедневные операции. Этот пробел в обучении сотрудников и культурном укреплении представляет собой критическое препятствие для МФО, стремящихся повысить свою киберустойчивость.

Исследования показывают, что атаки с использованием социальной инженерии являются одними из наиболее распространенных киберугроз, нацеленных на финансовые учреждения, включая МФО. Исследования Вишваната, Герата и Чена показали, что сотрудники финансовых учреждений часто не распознают фишинговые письма, которые обычно используются в атаках с использованием социальной инженерии. Исследование показало, что такие факторы, как рабочая нагрузка, отсутствие обучения и когнитивные предубеждения, повышают восприимчивость к этим атакам. Эти результаты свидетельствуют о том, что повышение осведомленности и обучения сотрудников имеет важное значение для снижения уязвимости к социальной инженерии, распространенной проблемы для МФО, работающих с ограниченными бюджетами на кибербезопасность.

Эмпирическое исследование, проведенное Уиллисоном и Уоркентином, было сосредоточено на внутренних угрозах в финансовых учреждениях, анализируя тематические исследования, чтобы понять, как организационная культура и контроль доступа сотрудников способствуют внутренним рискам. Исследование показало, что слабый внутренний контроль и отсутствие надзора создают возможности для



преднамеренных и непреднамеренных внутренних угроз. МФО из-за своей иерархической структуры и фокуса на доступности могут испытывать трудности с обеспечением строгого контроля доступа, таким образом оставаясь уязвимыми для внутренних угроз. Это исследование подтверждает необходимость для МФО устанавливать строгие политики контроля доступа и регулярного мониторинга для снижения внутренних рисков.

Исследование изучало влияние обучения по повышению осведомленности о кибербезопасности на снижение человеческих ошибок в небольших финансовых учреждениях, включая МФО. В исследовании опрашивались сотрудники из разных учреждений и было обнаружено, что специально разработанные программы обучения значительно снижают вероятность киберинцидентов, вызванных человеческими ошибками. Также было отмечено, что регулярное обучение и вовлечение высшего руководства играют жизненно важную роль в внедрении культуры кибербезопасности. Для МФО это исследование подчеркивает важность инвестирования в непрерывное обучение и развитие культуры киберосведомленности, даже если ресурсы ограничены.

Эти исследования в совокупности подчеркивают важную роль человеческого фактора в уязвимостях кибербезопасности в МФО. Они подчеркивают важность целевого обучения сотрудников, надежного внутреннего контроля и программ повышения осведомленности для снижения рисков. Результаты этих эмпирических исследований предлагают фундаментальное понимание для МФО, стремящихся разработать более эффективные стратегии защиты от киберугроз.

Выбранная литература была рассмотрена и классифицирована на основе тем, включая типы человеческих уязвимостей, проблемы, характерные для МФО, а также решения и передовой опыт. Основные выводы, методологии и заключения были обобщены, подчеркивая сходства, различия и пробелы в литературе. Литература была классифицирована по отдельным темам для облегчения структурированного анализа результатов. Этот подход позволил выявить повторяющиеся закономерности и темы, связанные с человеческими уязвимостями и проблемами кибербезопасности в МФО.

Были обобщены основные результаты каждого исследования, с акцентом на использованные методологии и последствия исследования для понимания уязвимостей человека в кибербезопасности. Тематический анализ был проведен для выявления общих закономерностей и тем, которые возникли в литературе, обеспечивая всестороннее понимание взаимодействия между человеческим фактором и кибербезопасностью в МФО.



В результате анализа в этом исследовании было получено 1357 записей. Перед проведением любого анализа первым шагом было устранение любых дубликатов записей. После удаления дубликатов осталось в общей сложности 1003 уникальных записи. Как предполагают Вайдт и Сильва (2016), первый шаг анализа включает в себя скрининг на основе заголовка и аннотации. В общей сложности 849 записей были признаны нерелевантными для этого обзора, в результате чего для дальнейшего скрининга было выбрано 154 статьи.

Вторая оценка включала анализ введения и заключения каждой статьи в зависимости от количества статей. На втором этапе отбора для этого исследования также была включена оценка раздела методологии. Это сократило общее количество до 57, а еще 97 статей были исключены из-за отсутствия эмпирических данных и несоответствия рассматриваемой теме, в результате чего окончательное количество статей для тщательного анализа текста составило 57. Адаптированный из Page *et al.*, процесс отбора проиллюстрирован на рисунке 1 ниже.

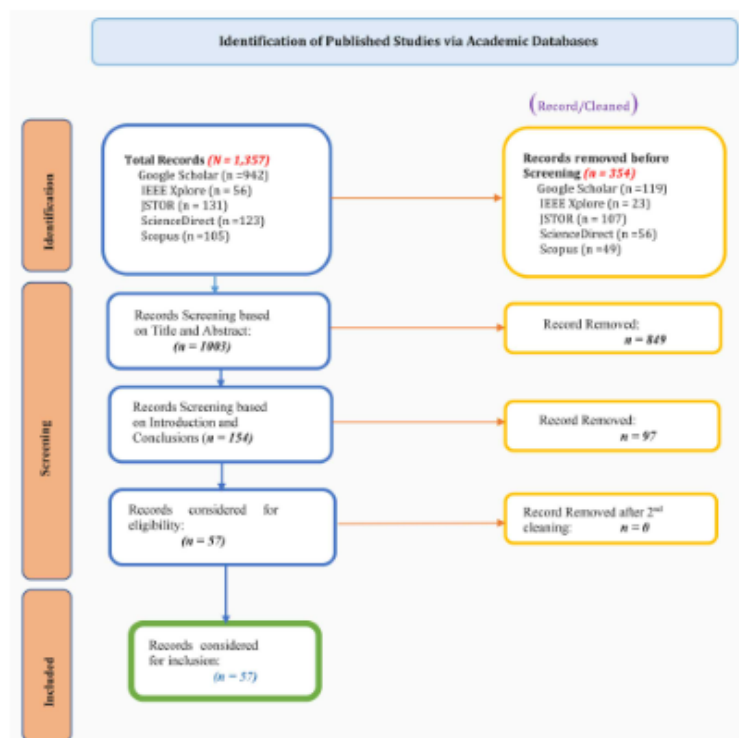


Рисунок 1. Отбор и включение записей в анализ.

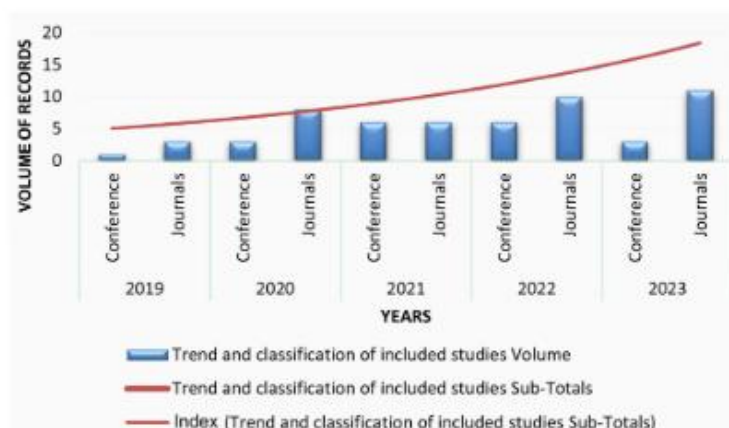


Рисунок 2. Тенденция и классификация включенных исследований.

Из 57 отобранных статей 38 были опубликованы в журналах, а остальные 9 — на конференциях, или 66,67% и 33,33% соответственно, как показано на рисунке 2. Рисунок также демонстрирует возросший интерес к теме за последние два года.

#### Задача 1: Анализ текущего ландшафта кибербезопасности в МФО

Анализ текущего ландшафта кибербезопасности в микрофинансовых организациях (МФО) из рассмотренных журналов показывает значительную распространенность киберугроз, поскольку 80% МФО сообщают о том, что подвергались атакам. Фишинг и социальная инженерия являются наиболее распространенными угрозами, регистрируя значительный рост на 65% и 40% соответственно с 2019 по 2023 год. Обзоры указали, что киберпреступники часто сосредотачиваются на сотрудниках с ограниченными знаниями в области кибербезопасности и используют их слабости.

Из 57 рассмотренных исследований в этом исследовании следует, что фишинговые атаки растут на 20% ежегодно с 2019 года и в первую очередь затрагивают неопытных младших сотрудников, которые не знают протоколы кибербезопасности. Кроме того, около 15% микрофинансовых организаций стали жертвами атак с использованием программ-вымогателей, направленных на доступ к конфиденциальным данным клиентов, что увеличивает риск, связанный с этими организациями. Около 70% микрофинансовых организаций полагаются на базовое антивирусное программное обеспечение и брандмауэры для обеспечения своей безопасности.

Только 30% выбирают более сложные меры, такие как многофакторная аутентификация и системы обнаружения угроз, как указано в 57 обзорных исследованиях.



Многие микрофинансовые организации сталкиваются с потенциальными угрозами как из внешних, так и из внутренних источников из-за разного уровня знаний в области безопасности. Одно из исследований, изучающих корреляцию между реализацией протоколов безопасности и инцидентами атак с использованием регрессионного анализа, показывает сильную обратную связь ( $R^2 = 0,65$ ), что говорит о том, что финансовые учреждения с улучшенными протоколами подвергаются меньшему количеству атак.

Задача 2: Выявление конкретных уязвимостей человека, способствующих киберугрозам

При изучении конкретных человеческих уязвимостей, способствующих киберугрозам в МФО, из 57 рассмотренных исследований для этого исследования было выявлено несколько ключевых проблем. Социальная инженерия была определена как наиболее распространенная уязвимость, при этом 74% исследований подчеркивали восприимчивость сотрудников к этой тактике. Эта уязвимость охватывает различные манипулятивные методы, включая фишинг и атаки с использованием маскировки, которые эксплуатируют доверие или неосведомленность сотрудников. Плохие методы использования паролей также распространены, при этом около 60% сотрудников МФО, как сообщается, повторно используют пароли в разных системах. В среднем сотрудник повторно использует приблизительно 3,2 балла по шкале от 1 до 5 паролей, что усиливает риск нарушений на основе учетных данных.

Еще одной значительной уязвимостью является отсутствие адекватного обучения по безопасности. Значительные 65% исследований назвали недостаточную подготовку фактором, способствующим этому, и только 40% МФО проводят ежегодные обучающие сессии по киберугрозам. Из-за отсутствия регулярного, целенаправленного обучения многие сотрудники оказываются неподготовленными к эффективному распознаванию и реагированию на киберриски.

Уязвимости также значительно различаются в зависимости от уровня сотрудников. Сотрудники начального уровня, из-за ограниченной грамотности в области кибербезопасности, демонстрируют самый высокий уровень уязвимости — 78%. Сотрудники среднего звена демонстрируют 60%-ную восприимчивость к методам социальной инженерии, в то время как сотрудники руководящего звена в первую очередь уязвимы из-за недостаточных знаний в области безопасной обработки данных — уровень уязвимости составляет 45%.



Задача 3: Оценка эффективности существующих программ обучения и повышения осведомленности.

Оценка существующих программ обучения и повышения осведомленности в МФО показывает различные уровни эффективности в зависимости от частоты, содержания и реализации этих инициатив. Среди исследованных МФО только 35% предлагают ежеквартальное обучение по безопасности, в то время как 65% либо проводят ежегодные сессии, либо вообще не проводят формальное обучение. МФО с ежеквартальным обучением сообщают о на 35% более низком уровне киберинцидентов, чем те, которые предлагают только ежегодные сессии, что указывает на положительное влияние регулярного обучения. Однако большинство программ (70%) сосредоточены на базовых темах, таких как управление паролями и осведомленность о фишинге, и только 30% охватывают продвинутые темы, такие как защита от социальной инженерии и реагирование на инциденты. Этот разрыв в объеме контента ограничивает общую эффективность этих программ.

С точки зрения изменения поведения сотрудников, частое обучение, по-видимому, значительно снижает уязвимость к фишинговым атакам. Сотрудники, участвующие в ежеквартальных сессиях, показали 50%-ное снижение восприимчивости к фишингу по сравнению с 20%-ным снижением среди тех, кто проходит ежегодное обучение. Статистический анализ с использованием парных t-тестов выявил существенное снижение киберинцидентов после обучения в МФО, которые реализуют частые и комплексные программы обучения ( $p < 0,01$ ), что подчеркивает ценность регулярного углубленного обучения, как обобщено в Таблице 1 ниже.



Таблица 1. Резюме результатов.

Цель	Основные выводы	Статистический анализ
<b>1. Анализ текущего ландшафта кибербезопасности</b>	<ul style="list-style-type: none"><li>- 80% МФО сообщили о киберугрозах, при этом на 65% увеличилось количество фишинговых атак, а на 40% — количество атак с использованием социальной инженерии (2019–2023 гг.).</li><li>- 30% МФО используют передовые протоколы безопасности.</li></ul>	<ul style="list-style-type: none"><li>- Ежегодный рост фишинговых атак на сотрудников составил 20%.</li><li>- Регрессионный анализ (<math>R^2 = 0,65</math>) показывает, что более высокий уровень внедрения мер безопасности значительно снижает количество случаев атак.</li></ul>
<b>2. Выявление конкретных уязвимостей человека</b>	<ul style="list-style-type: none"><li>- 74% МФО уязвимы для социальной инженерии; уровень повторного использования паролей высок (60%).</li><li>- Наибольшая уязвимость наблюдается у сотрудников начального уровня (78%), среднего звена (60%), руководства (45%).</li></ul>	<ul style="list-style-type: none"><li>- ANOVA выявил значительные различия в уязвимости между уровнями сотрудников (<math>p &lt; 0,05</math>).</li></ul>
<b>3. Оценка эффективности программ обучения</b>	<ul style="list-style-type: none"><li>- Только 35% МФО проводят ежеквартальное обучение; 65% проводят ежегодное обучение или не проводят его вообще.</li><li>- Ежеквартальное обучение снижает уязвимость к фишингу на 50% по сравнению с 20% при ежегодном обучении.</li></ul>	<ul style="list-style-type: none"><li>- Парный t-тест подтверждает значительное снижение числа инцидентов после обучения (<math>p &lt; 0,01</math>).</li></ul>

Результаты программы повышения осведомленности демонстрируют неоднозначные результаты в сохранении и применении знаний. Из Таблицы 1 видно, что 60% сотрудников хорошо усвоили содержание обучения, но только 45% последовательно применяли эти знания в повседневной работе, что указывает на разрыв между пониманием концепций кибербезопасности и их практикой в реальных сценариях. Этот разрыв подчеркивает необходимость более интерактивных, основанных на моделировании учебных сессий для закрепления практического применения. Кроме того, исследования экономической эффективности показывают, что МФО экономят в 1,5 раза больше затрат на реализацию мер безопасности на одного сотрудника за счет снижения уязвимостей с помощью эффективного обучения, подчеркивая финансовую выгоду от инвестирования в надежное образование в области кибербезопасности.

**Заключение:** Исследование показывает, что нехватка ресурсов в микрофинансовых организациях (МФО) влияет на их способность предлагать тщательное обучение и инфраструктуру, что приводит к уязвимости человека, что является важнейшим аспектом рисков кибербезопасности. Недавно нанятые сотрудники уязвимы для кибератак из-за отсутствия знаний о таких опасностях, как фишинг и социальная инженерия. Неадекватное обучение препятствует использованию расширенных мер безопасности, таких как многофакторная аутентификация, и подвергает МФО внутренним и внешним рискам.

Ограниченное финансирование препятствует непрерывному обучению и созданию надежной системы кибербезопасности. Если МФО не отдадут приоритет стратегическому



обучению и использованию ресурсов, это может привести к постоянной уязвимости кадровых ресурсов, подвергая конфиденциальные данные клиентов риску кибератак. Исследование подчеркивает важность улучшения образования в области кибербезопасности и финансирования проактивных технологий для эффективного снижения рисков.

### **Литература:**

1. Штеренберг С. И., Бударный Г. С., Чумаков И. В. Анализ безопасности доменных систем //Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская. – 2022. – С. 587.
2. Бударный Г. С., Камалова А. О., Красов А. В. СРАВНЕНИЕ СТАТИЧЕСКОГО И ДИНАМИЧЕСКОГО АНАЛИЗА КОДА И ИХ РОЛЬ В МЕТОДОЛОГИИ DEVSECOPS //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 204-208.
3. Штеренберг С. И., Бударный Г. С., Чумаков И. В. Методика обеспечения безопасности доменных систем доверенной зоны //Региональная информатика и информационная безопасность. – 2022. – С. 621-625.
4. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем //Транспортное машиностроение. – 2020. – №. 3 (88). – С. 38-46.
5. Гельфанд А. М. и др. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.



Масликов Тимофей Олегович

Студент 5 курс, факультет КБ

Институт телекоммуникаций им. проф. М.А. Бонч-Бруевича

## ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ И ТЕХНОЛОГИЧЕСКАЯ ИНТЕГРАЦИЯ В ЦЕПОЧКЕ ПОСТАВОК ВОЕННОГО НАЗНАЧЕНИЯ 4.0

Аннотация: Концепция Supply Chain 4.0 представляет собой преобразующую фазу в управлении цепочками поставок с помощью передовых цифровых технологий, таких как IoT, AI, блокчейн и киберфизические системы. Хотя эти инновации обеспечивают операционные улучшения, повышенная взаимосвязанность создает значительные проблемы кибербезопасности, особенно в военной логистике, где критически важные операции и проблемы безопасности жизни имеют первостепенное значение. В этой статье рассматриваются эти уникальные требования кибербезопасности, уделяя особое внимание продвинутым постоянным угрозам, отравлению цепочек поставок и утечкам данных, которые могут поставить под угрозу конфиденциальные операции. В исследовании предлагается гибридная структура кибербезопасности, адаптированная к военной логистике, объединяющая устойчивость, избыточность и меры безопасности между юрисдикциями. Применимость в реальном мире подтверждается с помощью моделирования, предлагающего стратегии для обеспечения безопасности цепочек поставок при одновременном балансе безопасности, эффективности и гибкости.

*Ключевые слова:* Кибербезопасность , Цепочка поставок , Интернет вещей , Блокчейн , Искусственный интеллект, Информационная безопасность, СПбГУТ им. Проф. Бонч-Бруевича.

*Keywords:* Cybersecurity, Supply Chain, IoT, BlockChain, Artificial Intelligence, Information security, SPbSUT im. Prof. Bonch-Bruevich.

Военные цепочки поставок принципиально отличаются от гражданских аналогов, отдавая приоритет устойчивости, гибкости и обеспечению выполнения миссии, а не экономической эффективности и оптимизированным операциям. Например, датчики IoT могут отслеживать критически важное военное оборудование в режиме реального времени, но они также создают уязвимости для продвинутых постоянных угроз (APT), с



которыми гражданские цепочки поставок могут не сталкиваться. Динамичный ландшафт угроз в военной логистике требует надежных структур кибербезопасности, которые учитывают риски для безопасности жизни, непредсказуемость операций и враждебные намерения. Эти проблемы усиливают потребность в критически важных технологиях, которые повышают оперативность реагирования и одновременно смягчают уязвимости.

Supply Chain 4.0 олицетворяет интеграцию физических и цифровых активов в сети цепочки поставок, используя технологии Industry 4.0 для обеспечения интеллектуальных, взаимосвязанных логистических систем, которые работают независимо от временных или пространственных ограничений. Эта интеграция облегчает широкий спектр функций — от автоматизированного управления запасами до отслеживания логистики в реальном времени и прогнозной аналитики спроса, — которые оптимизируют эффективность и адаптивность цепочки поставок. Ключевые компоненты Supply Chain 4.0, как показано на рисунке 1, включают в себя передовые устройства IoT, сети на основе блокчейна, аналитику на основе ИИ и облачную инфраструктуру, каждый из которых играет важную роль в оптимизации логистических процессов и обеспечении принятия решений в реальном времени. Однако переход от традиционных цепочек поставок к цифровым сетевым системам создает уникальные риски кибербезопасности, поскольку растущая зависимость от IoT, блокчейна и ИИ создает новые уязвимости в инфраструктуре цепочки поставок/

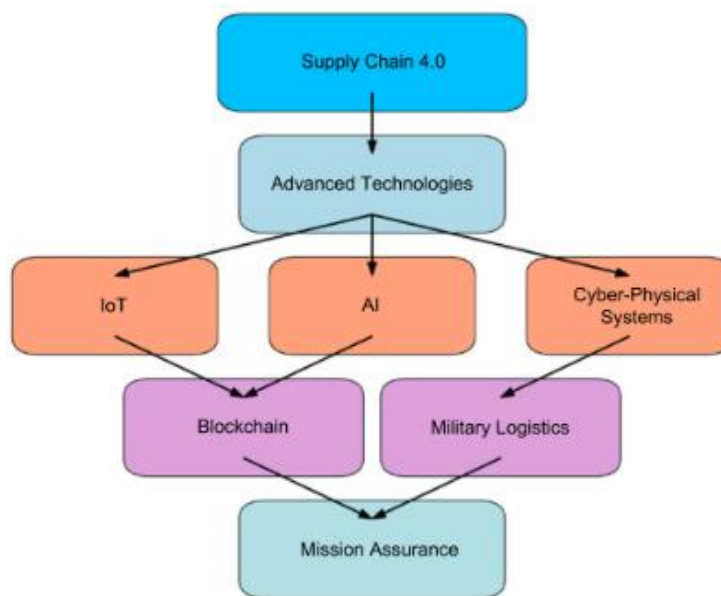


Рисунок 1. Компоненты цепочки поставок 4.0.

Военные цепочки поставок, учитывая их стратегическую важность, значительно отличаются от гражданских приложений как по оперативной направленности, так и по потребностям безопасности. Гражданские цепочки поставок обычно отдают приоритет эффективности и рентабельности, в то время как военная логистика сосредоточена на устойчивости, гибкости и обеспечении выполнения миссии. Киберфизические системы (CPS) и устройства IoT, используемые в Supply Chain 4.0, повышают оперативность и оптимизируют логистические процессы в военных операциях, но они также открывают критические уязвимости, которые противники могут использовать для нарушения операций или компрометации конфиденциальных данных. Уникальные уязвимости, создаваемые военными цепочками поставок, проистекают из высокой связанности систем Supply Chain 4.0, которые могут подвергать эти сети воздействию Advanced Persistent Threats (APT) и других сложных кибератак. Военные цепочки поставок управляют потоком жизненно важных ресурсов, оборудования и персонала, необходимых для успеха миссии, что делает кибербезопасность центральным фактором. В то время как гражданские цепочки поставок сталкиваются с аналогичными рисками, последствия нарушений в военной логистике выходят за рамки финансовых потерь и могут поставить под угрозу человеческие жизни и национальную безопасность. Следовательно, военные цепочки поставок требуют стратегий кибербезопасности, которые учитывают как



операционную непрерывность, так и динамический ландшафт угроз. Supply Chain 4.0 представляет собой цифровую трансформацию традиционных цепочек поставок посредством интеграции передовых технологий, таких как Интернет вещей (IoT), искусственный интеллект (AI), киберфизические системы и блокчейн. Эти технологии предлагают различные усовершенствования, включая аналитику данных в реальном времени, автоматизацию и возможности автономного принятия решений, которые повышают эффективность, оперативность и точность цепочки поставок. Концепция возникла из Industry 4.0, которая фокусируется на интеллектуальном производстве, автоматизации и применении взаимосвязанных систем, что позволяет организациям переходить от изолированных операций к интегрированным, сквозным цифровым сетям. В этом контексте Supply Chain 4.0 является ключевой трансформацией, переопределяющей то, как материалы, товары и информация управляются и обмениваются по всему континууму цепочки поставок.

Для военного сектора Supply Chain 4.0 имеет важное значение не только для оптимизации логистических функций, но и для обеспечения гарантии выполнения миссии и оперативной готовности. Военные цепочки поставок управляют перемещением критически важных ресурсов, от систем вооружения до основных товаров для персонала, в условиях, которые часто требуют быстрой адаптации и устойчивости. В отличие от гражданских цепочек поставок, которые отдают приоритет экономической эффективности и оптимизированным операциям, военные цепочки поставок подчеркивают гибкость, безопасность и избыточность для поддержки динамических оперативных потребностей. Интегрируя датчики с поддержкой IoT, аналитику на основе ИИ и прослеживаемость на основе блокчейна, военная логистика может повысить точность инвентаризации, оптимизировать процессы и получить повышенную прозрачность маршрутов поставок. Такие достижения позволяют военным организациям лучше управлять непредсказуемым спросом и сложной логистикой в нестабильных условиях.

Внедрение технологий Supply Chain 4.0 в военную логистику также способствует улучшению взаимодействия между союзными странами. Многие военные операции сегодня опираются на партнерства и коалиции, что делает крайне важным, чтобы цепочки поставок функционировали бесперебойно в разных системах и юрисдикциях. Стандартизация и взаимодействие, обеспечиваемые Supply Chain 4.0, облегчают сотрудничество между союзными силами, улучшая логистическую координацию и сокращая узкие места в доставке ресурсов. Кроме того, решения IoT и AI предоставляют



возможности предиктивной аналитики, которые бесценны для прогнозирования дефицита поставок, поддержания баланса запасов и прогнозирования логистических потребностей.

Цифровая трансформация цепочек поставок создает новые уязвимости, поскольку организации становятся все более зависимыми от взаимосвязанных цифровых систем. Угрозы кибербезопасности, такие как Advanced Persistent Threats (АРТ), утечки данных и атаки программ-вымогателей, являются распространенными рисками, связанными с высокой степенью связности сетей Supply Chain 4.0. АРТ, например, позволяют злоумышленникам проникать в системы цепочек поставок в течение длительных периодов времени, собирать разведданные и потенциально нарушать операции без немедленного обнаружения. Растущее использование устройств IoT, которые часто не имеют надежных функций безопасности, еще больше увеличивает эти риски, расширяя поверхность атаки и создавая точки входа для кибервторжений.

Отравление цепочки поставок является особенно тревожным риском в военных контекстах, где противники могут скомпрометировать критические компоненты на различных этапах цепочки поставок. Эти скомпрометированные компоненты могут проникнуть в защищенные военные среды, потенциально ставя под угрозу конфиденциальные данные и операционную целостность. Кроме того, интеграция блокчейна и ИИ в Supply Chain 4.0, предлагая повышенную прозрачность данных и возможности прогнозирования, создает новые проблемы кибербезопасности. Например, технология блокчейн подвержена определенным атакам, таким как «атака 51%», когда злоумышленники могут взять под контроль сеть блокчейнов, ставя под угрозу целостность данных. Системы ИИ, особенно те, которые развернуты в автономных логистических операциях, уязвимы для враждебных атак, которые могут манипулировать входными данными, что приводит к ошибочному принятию решений или сбоям в автоматизированных процессах.

Зависимость от цифровых и сетевых систем также создает проблемы, связанные с конфиденциальностью информации и устойчивостью системы. Концепция «безопасности через неизвестность», когда военные сети полагаются на ограниченное воздействие публичных сетей, больше не является достаточной в эпоху взаимосвязанных цепочек поставок. В ответ военные организации принимают надежные структуры кибербезопасности, которые включают принципы управления рисками для упреждающего выявления и смягчения уязвимостей в операциях цепочки поставок. Эти структуры жизненно важны для обеспечения того, чтобы военная логистика оставалась безопасной,



устойчивой и реагировала на возникающие угрозы как в киберпространстве, так и в физическом мире.

### **Адаптация гражданских фреймворков для военных приложений**

Эффективное управление рисками имеет жизненно важное значение для снижения рисков кибербезопасности, присущих Supply Chain 4.0. Гражданские структуры, такие как модель Cyber Supply Chain Risk Management (CSCRM), подчеркивают комплексный подход к жизненному циклу, оценивая уязвимости от проектирования до развертывания. Хотя эти модели предлагают ценные идеи, военная логистика требует усовершенствований, таких как меры обеспечения миссии и возможности быстрого реагирования на инциденты для устранения жизненно важных последствий сбоев в цепочке поставок.

Cyber **Kill Chain**, разработанный Lockheed Martin, отображает этапы кибератаки, позволяя организациям обнаруживать и пресекать угрозы.

Аналогичным образом, модель **Supply Chain Operations Reference (SCOR)** предлагает структурированный процесс оптимизации производительности цепочки поставок по пяти ключевым направлениям: планирование, источник, производство, доставка и возврат. Несмотря на ценность для достижения эффективности и качества, модель SCOR требует изменений для удовлетворения специфических военных потребностей в кибербезопасности. К ним относятся меры по обеспечению устойчивости для защиты от киберинцидентов и обеспечения непрерывности критически важных цепочек поставок во время враждебных событий.

### **Конкретные военные рамки устойчивости**

**В рамках концепции устойчивости Петгита, Фикселя и Крокстона подчеркиваются такие возможности, как гибкость, избыточность и восстановление, которые имеют решающее значение для военных цепочек поставок, работающих в нестабильных и враждебных условиях. Например, диверсифицированный источник поставок, мониторинг в реальном времени и планирование на случай непредвиденных обстоятельств защищают от сбоев, вызванных кибер- или физическими угрозами.**

Военные цепочки поставок должны включать гибридный подход, который сочетает эффективность процесса гражданских структур с военными стратегиями. Эта гибридная модель объединяет такие элементы, как:

**1) Планирование избыточности:** резервные поставщики, альтернативные каналы сбыта и буферные запасы.



**2) Проактивная оценка рисков** : выявление потенциальных уязвимостей на всех этапах жизненного цикла цепочки поставок.

**3) Адаптивность в реальном времени** : быстрое обнаружение и устранение угроз с использованием аналитики на основе искусственного интеллекта и мониторинга с использованием Интернета вещей.

Например, адаптированная адаптация Cyber Kill Chain могла бы интегрировать предиктивную аналитику для систем раннего оповещения, позволяя военным логистикам противостоять Advanced Persistent Threats (APT) до того, как они обострятся. Аналогичным образом, модель SCOR может быть улучшена системами разведки угроз в реальном времени для поддержания целостности цепочки поставок во время киберсобытий.

### **Вклады и будущие направления**

Это исследование расширяет рамки управления гражданскими рисками для удовлетворения оперативных потребностей военной логистики, устраняя пробелы в адаптивности, устойчивости и обеспечении миссии. Интегрируя планирование избыточности, кросс-функциональную совместимость и передовые протоколы кибербезопасности, предлагаемый гибридный подход гарантирует, что военные цепочки поставок остаются безопасными и работоспособными даже перед лицом развивающихся киберугроз. Будущие исследования должны изучить дополнительные приложения ИИ и блокчейна для дальнейшего повышения устойчивости и разработки кросс-юрисдикционных стандартов для союзнических операций.

Военная логистика все больше полагается на передовые технологии, такие как IoT, блокчейн и ИИ для мониторинга в реальном времени, предиктивной аналитики и отслеживания активов. Эти технологии повышают эффективность и устойчивость цепочки поставок, но также вносят уникальные проблемы кибербезопасности, которые необходимо решать проактивно.

### **Интернет вещей в военной логистике**

Устройства с поддержкой IoT предлагают значительные преимущества, такие как предиктивное обслуживание, которое обеспечивает эксплуатационную готовность путем выявления потенциальных сбоев оборудования до того, как они произойдут. Например, мониторинг узлов цепочки поставок в реальном времени может обнаруживать и предупреждать логистов о нарушениях в транспортных маршрутах или условиях окружающей среды. Однако устройствам IoT часто не хватает надежных протоколов



безопасности, что делает их уязвимыми для атак, таких как захват устройств, манипулирование данными и подмена сигналов. Обеспечение безопасности сетей IoT в военных контекстах включает внедрение шифрования, сегментации сети и мониторинга угроз в реальном времени для предотвращения несанкционированного доступа и обеспечения целостности данных.

### **Блокчейн для прозрачности и отслеживаемости**

Блокчейн обеспечивает децентрализованный, защищенный от несанкционированного доступа реестр, который регистрирует каждую транзакцию в цепочке поставок. Это повышает прослеживаемость и прозрачность, делая его бесценным для военной логистики, где поддельные товары или отравление цепочки поставок представляют собой критические риски. Например, блокчейн может отслеживать жизненный цикл компонентов от производства до развертывания, обеспечивая подлинность и снижая уязвимости. Однако зависимость блокчейна от механизмов консенсуса создает проблемы, такие как риск атаки 51%, когда злоумышленники получают контроль над сетью. Чтобы решить эти проблемы, военные приложения должны использовать разрешенные системы блокчейнов с многоуровневой аутентификацией и передовыми протоколами шифрования, адаптированными к чувствительным эксплуатационным потребностям.

### **ИИ и машинное обучение для прогнозирования**

Технологии на основе ИИ позволяют проводить предиктивную аналитику, прогнозировать спрос и оптимизировать распределение ресурсов в Supply Chain 4.0. Эти инструменты могут выявлять закономерности в логистических данных, предвидеть сбои и оптимизировать процессы принятия решений. Однако враждебные атаки на алгоритмы ИИ представляют серьезную угрозу для военной логистики, поскольку манипулирование входными данными может привести к неверным выводам или системным сбоям. Чтобы смягчить эти угрозы, военные цепочки поставок должны внедрять строгое тестирование, частые обновления моделей машинного обучения и комплексные процессы проверки и валидации, учитывающие враждебные сценарии.

### **Киберфизические системы (CPS) для оперативного управления**

Киберфизические системы (CPS) интегрируют цифровые и физические процессы, обеспечивая удаленный контроль и мониторинг активов военной цепочки поставок. Эти системы играют важную роль в поддержании оперативной готовности и устойчивости. Однако CPS уязвимы для междоменных угроз, таких как подмена GPS, глушение



сигналов и физическое вмешательство. Эффективные стратегии смягчения включают развертывание многоуровневых защитных механизмов, обнаружение аномалий в реальном времени и планирование избыточности. Эти меры гарантируют, что как цифровые, так и физические компоненты CPS защищены от сбоев.

Интегрируя эти технологии с индивидуальными решениями в области кибербезопасности, военная логистика может извлечь выгоду из операционной эффективности Supply Chain 4.0, сохраняя при этом устойчивость и гарантию выполнения задач перед лицом постоянно меняющихся киберугроз.

Разведка угроз и мониторинг в реальном времени : центральное место в структуре занимает система непрерывного мониторинга, поддерживаемая датчиками IoT и аналитикой данных в реальном времени. Эти инструменты поддерживают раннее обнаружение угроз и быстрое реагирование, позволяя военным логистическим операциям оставаться устойчивыми даже во время активных киберугроз. Прогностические модели на основе ИИ анализируют входящие данные для прогнозирования потенциальных рисков, в то время как алгоритмы машинного обучения выявляют аномальные закономерности, указывающие на возникающие угрозы.

Планирование устойчивости и избыточности : Основываясь на аспектах устойчивости модели SCOR, эта структура включает избыточность в ключевых узлах цепочки поставок, обеспечивая непрерывность работы даже в случае нарушения основных узлов. Это включает в себя установление альтернативных поставщиков, поддержание буферных запасов и создание планов действий в чрезвычайных ситуациях для критических компонентов, таких как системы вооружения или устройства связи.

Протоколы безопасности между юрисдикциями : военные операции часто требуют сотрудничества через национальные границы и между союзными силами. Предлагаемая структура включает меры безопасности между юрисдикциями, такие как стандартизированные протоколы шифрования и защищенные каналы связи. Эти протоколы гарантируют, что конфиденциальные данные остаются в безопасности во время многонациональных логистических операций и способствуют взаимодействию между союзными силами.

Процесс валидации : Рисунок 2 показывает разработку и валидацию фреймворка. Надежность и применимость фреймворка оценивались с помощью экспертных обзоров и моделирования примеров. Сценарии, основанные на прошлых военных киберинцидентах, были смоделированы для проверки эффективности фреймворка в условиях активных



киберугроз, что дало представление о областях, где могут потребоваться корректировки или дополнительные меры. Благодаря сравнительному анализу с устоявшимися фреймворками и включению отзывов из реального мира предлагаемая модель демонстрирует повышенную устойчивость и адаптивность к киберрискам, тем самым усиливая ее полезность в военной логистике.

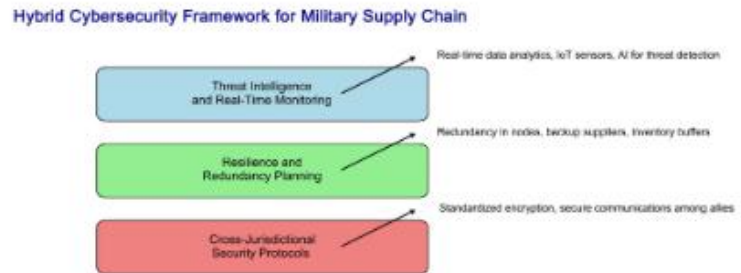


Рисунок 2. Разработка и проверка фреймворка.

Для повышения надежности и применимости предлагаемой структуры была использована многогранная стратегия проверки, сочетающая в себе моделируемые примеры, экспертные обзоры и сравнительный анализ с устоявшимися моделями.

### Моделирование практических примеров

Имитационные сценарии, смоделированные на основе исторических киберинцидентов, таких как атака Stuxnet, демонстрируют эффективность фреймворка в борьбе с реальными угрозами. В одном из сценариев злоумышленники проникли на маршруты поставок и подделали военное оборудование на пути к развертыванию. Система мониторинга в реальном времени и обнаружения аномалий фреймворка выявила нарушения в данных о поставках, такие как отклонения в транзитных путях и неожиданные задержки. Это вызвало немедленные корректирующие действия, включая изоляцию скомпрометированного узла цепочки поставок и перенаправление незатронутых активов для поддержания непрерывности работы.

В другом моделировании атака 51% на систему отслеживания активов на основе блокчейна была предотвращена многоуровневыми защитными механизмами фреймворка, включавшими контроль разрешенного доступа и расширенные протоколы аутентификации. Эти меры гарантировали, что скомпрометированные узлы были изолированы без нарушения общей работы цепочки поставок.

### Экспертные обзоры



Предложенная структура была рассмотрена экспертами по кибербезопасности и военной логистике для обеспечения практической релевантности и соответствия реальным оперативным потребностям. Эксперты подчеркнули важность включения возможностей быстрого реагирования на инциденты и постоянного тестирования предиктивной аналитики на основе ИИ для реагирования на меняющиеся ландшафты угроз. Обратная связь по этим обзорам была включена в структуру, что улучшило ее компоненты и повысило ее адаптивность к военной логистике с высокими ставками.

### **Сравнительный анализ**

Для дальнейшей проверки эффективности фреймворка он был сравнен с существующими гражданскими и военными моделями кибербезопасности, такими как Cyber Kill Chain и модель SCOR. Этот сравнительный анализ подчеркнул сильные стороны фреймворка в решении военных специфических требований, включая кросс-юрисдикционную совместимость, обеспечение миссии и адаптивность в реальном времени. Например, в то время как Cyber Kill Chain предоставил основополагающие идеи по срыву векторов атак, предлагаемый фреймворк продемонстрировал превосходную устойчивость за счет включения избыточности и проактивного управления рисками, адаптированного к военным цепочкам поставок.

Военные цепочки поставок, неотъемлемые для готовности к миссии и оперативного успеха, сталкиваются с рядом угроз кибербезопасности, усугубляемых расширенной связностью Supply Chain 4.0. Эта улучшенная связность, хотя и полезна для эффективности и мониторинга в реальном времени, открывает новые уязвимости для эксплуатации. Кибератаки, нацеленные на военные цепочки поставок, выходят за рамки типичных нарушений данных; они охватывают как цифровые вторжения, так и физическое вмешательство, в совокупности именуемое «отравлением цепочки поставок». Злоумышленники могут перехватывать поставки и вмешиваться в критически важные компоненты, которые, будучи встроенными в военные активы, могут привести к катастрофическим сбоям в работе. Например, злоумышленники могут проникнуть в цепочку поставок, вставив скомпрометированное оборудование в основные системы, что, если их не обнаружить, может нарушить связь, помешать системам вооружения или даже разрешить несанкционированный удаленный доступ.

Такие вторжения ставят под угрозу критически важные активы и создают значительные риски для военнослужащих, подчеркивая необходимость строгих мер кибербезопасности на всех этапах цепочки поставок. Этот ландшафт угроз, включающий



как прямые кибератаки, так и косвенное отравление цепочки поставок, подчеркивает необходимость расширенного мониторинга и механизмов сквозной защиты в военных сетях поставок. Эти защитные меры должны также распространяться на сторонних поставщиков и подрядчиков, которые часто становятся целью злоумышленников как точка входа. Риски, связанные даже с незначительными уязвимостями цепочки поставок, заставили военные организации отдать приоритет всеобъемлющим протоколам безопасности, адаптированным к их уникальным эксплуатационным требованиям. Следующий график на рисунке 3 иллюстрирует относительную распространенность и серьезность различных уязвимостей кибербезопасности, влияющих на военную логистику. Выделяя эти уязвимости, этот анализ подчеркивает области, в которых надежные стратегии кибербезопасности наиболее необходимы.

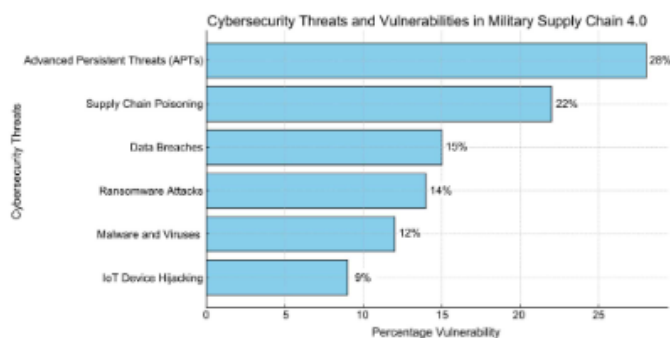


Рисунок 3. Уникальные угрозы кибербезопасности в цепочке поставок военной продукции.

**Заключение:** Это исследование показывает, что, хотя технологии Supply Chain 4.0 предлагают беспрецедентную эффективность и прозрачность, они вносят критические уязвимости, которые необходимо устранить в военной логистике. Предлагаемая гибридная структура устраняет разрыв между гражданскими и военными, объединяя эффективность процессов со специфическими для обороны мерами, такими как избыточность и адаптивность в реальном времени. Основные выводы подчеркивают необходимость многоуровневого подхода к обеспечению безопасности военных цепочек поставок, который объединяет мониторинг в реальном времени, планирование избыточности и протоколы безопасности между юрисдикциями. Предлагаемая структура, подтвержденная с помощью отзывов экспертов и смоделированных примеров, демонстрирует улучшенную адаптивность к киберугрозам, подчеркивая важность адаптированных военных стандартов кибербезопасности. Будущие исследования должны



быть сосредоточены на масштабировании блокчейна для крупномасштабных военных приложений и совершенствовании обнаружения угроз на основе ИИ для адаптации к меняющимся киберрискам. Эти инновации необходимы для поддержания непрерывности миссии и защиты национальной безопасности во все более взаимосвязанном цифровом ландшафте.

#### Литература:

1. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
2. Шариков П. И., Красов А. В., Штеренберг С. И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов //Т-Comm-Телекоммуникации и Транспорт. – 2017. – Т. 11. – №. 3. – С. 66-70.
3. Сахаров Д. В. и др. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 //Защита информации. Инсайд. – 2020. – №. 1. – С. 51-57.
4. Красов А. В., Шариков П. И. Методика защиты байт-кода Java-программы от декомпиляции и хищения исходного кода злоумышленником //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2017. – №. 1. – С. 47-50.
5. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.



Земцов Данила Сергеевич

Студент 5 курс, факультет КБ

Университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

## ПЕРЕСЕЧЕНИЕ КОНЦЕПЦИИ КОНФИДЕНЦИАЛЬНОСТИ ПО ЗАМЫСЛУ И ПОВЕДЕНЧЕСКОЙ ЭКОНОМИКИ: ПОДТАЛКИВАНИЕ ПОЛЬЗОВАТЕЛЕЙ К ВЫБОРУ, БЛАГОПРИЯТНОМУ ДЛЯ КОНФИДЕНЦИАЛЬНОСТИ

Аннотация: В этой статье проводится всесторонний обзор существующих исследований по теме Privacy by Design (PbD) и поведенческой экономики, изучается пересечение Privacy by Design (PbD) и поведенческой экономики, а также то, как дизайнеры могут использовать «подталкивания», чтобы поощрять пользователей к выбору, благоприятному для конфиденциальности. Мы анализируем ограничения рационального выбора в контексте принятия решений о конфиденциальности и определяем ключевые возможности для интеграции поведенческой экономики в PbD. Мы предлагаем ориентированную на пользователя структуру проектирования для интеграции поведенческой экономики в PbD, которая включает стратегии упрощения сложного выбора, обеспечения видимости конфиденциальности, предоставления обратной связи и контроля, а также тестирования и итерации. Наш анализ подчеркивает необходимость более тонкого понимания поведения пользователя и принятия решений в контексте конфиденциальности и демонстрирует потенциал поведенческой экономики для информирования о разработке более эффективных решений PbD.

*Ключевые слова:* конфиденциальность по замыслу, Поведенческая экономика, Подталкивания, Дизайн, ориентированный на пользователя, Защита данных, Когнитивные искажения, Эвристика, СПбГУТ им. Проф. Бонч-Бруевича.

*Keywords:* privacy by Design, Behavioral Economics, Nudges, User-Centered Design, Data Protection, Cognitive Biases, Heuristics, SPbSUT im. Prof. Bonch-Bruevich.

Растущая зависимость от цифровых технологий привела к растущей обеспокоенности по поводу конфиденциальности пользователей. Чтобы решить эту проблему, Privacy by Design (PbD) стала важнейшей основой для проектирования систем и



продуктов, которые отдают приоритет конфиденциальности пользователей. PbD основана на семи принципах, включая:

- 1) Проактивный, а не реактивный; превентивный, а не исправительный;
- 2) Конфиденциальность как настройка по умолчанию;
- 3) Конфиденциальность, заложенная в дизайн;
- 4) Полная функциональность — с положительной суммой, а не с нулевой;
- 5) Сквозная безопасность — защита на протяжении всего жизненного цикла;
- 6) Видимость и прозрачность — сохраняйте открытость;
- 7) Уважайте конфиденциальность пользователей — ориентируйтесь на их интересы.

Эти принципы направлены на то, чтобы гарантировать, что конфиденциальность пользователя учитывается на каждом этапе процесса проектирования, от начальной фазы проектирования до развертывания и обслуживания системы или продукта. Однако существующие исследования показали, что эффективность PbD в значительной степени зависит от принятия пользователями обоснованных решений о своих настройках конфиденциальности. К сожалению, исследования в области поведенческой экономики показали, что люди склонны к когнитивным предубеждениям и эвристике, что приводит к неоптимальному выбору, который ставит под угрозу их конфиденциальность.

Целью данной статьи является решение следующих проблем:

- Как дизайнеры могут использовать поведенческую экономику, чтобы побудить пользователей делать выбор, учитывающий требования конфиденциальности?
- Каковы ограничения существующих решений PbD в плане учета психологических и социальных факторов, влияющих на принятие решений пользователем?
- Как можно улучшить PbD, чтобы учесть когнитивные предубеждения и эвристику, влияющие на выбор пользователя?

Исследуя пересечение PbD и поведенческой экономики, в данной статье предлагается структура для интеграции поведенческой экономики в PbD с целью создания более эффективных и ориентированных на пользователя решений PbD.

Поведенческая экономика изучает, как психологические, социальные и эмоциональные факторы влияют на экономические решения. В контексте PbD поведенческая экономика может помочь дизайнерам понять, как пользователи принимают решения о своих настройках конфиденциальности. Например:



- Предвзятость по умолчанию: пользователи склонны придерживаться настроек по умолчанию, даже если это ставит под угрозу их конфиденциальность.
- Эффекты фрейминга: на решения пользователей влияет способ представления информации, а не сама информация.
- Неприятие потерь: пользователи боятся потерь больше, чем ценят выгоды, что приводит к поведению, не склонному к риску.
- Персонализация: изучите, как можно разработать персонализированные подсказки, учитывающие предпочтения и поведение отдельных пользователей, повышая эффективность выбора, учитывающего конфиденциальность.
- Эмоциональные призывы: изучите роль эмоций в принятии решений и то, как дизайнеры могут использовать эмоциональные призывы, чтобы подтолкнуть пользователей к выбору, учитывающему конфиденциальность.
- Культурные факторы: изучите влияние культурных факторов на решения пользователей относительно конфиденциальности и то, как дизайнеры могут адаптировать подталкивания для учета различных культурных контекстов.

Чтобы преодолеть эти предубеждения, дизайнеры могут использовать «подталкивания» — тонкие изменения в среде, которые влияют на поведение пользователей, не ограничивая их свободу выбора. Вот несколько примеров подталкиваний, которые могут способствовать выбору, благоприятному для конфиденциальности:

- Настройки конфиденциальности по умолчанию: установите настройки по умолчанию, чтобы отдать приоритет конфиденциальности пользователя, например, отказаться от сбора данных или использовать сквозное шифрование.
- Визуальные подсказки: используйте понятный, лаконичный язык и визуальные индикаторы, чтобы подчеркнуть потенциальные риски для конфиденциальности, помогая пользователям более осознанно делать свой выбор.
- Механизмы обратной связи: Предоставьте пользователям обратную связь по их настройкам конфиденциальности, например, «оценку конфиденциальности» или панель мониторинга, отображающую активность обмена данными.
- Социальные нормы: используйте социальные нормы, показывая количество пользователей, которые решили отдать приоритет своей конфиденциальности, и побуждая других последовать их примеру.



- Динамическое подталкивание: разрабатывайте подталкивания, которые со временем адаптируются к поведению пользователей, обеспечивая персонализированную обратную связь и поощрение.
- Социальное влияние: исследуйте роль социального влияния в формировании решений пользователей относительно конфиденциальности и разрабатывайте подталкивания, которые используют социальные сети для поощрения выбора, благоприятного для конфиденциальности.
- Геймификация: изучите использование элементов геймификации, таких как награды и испытания, чтобы сделать выбор, учитывающий конфиденциальность, более интересным и приятным.

Мы предлагаем структуру для интеграции поведенческой экономики в PbD, включающую следующие стратегии:

- 1) Упростите сложный выбор: разбейте сложные решения по вопросам конфиденциальности на простые и выполнимые варианты.
- 2) Сделайте конфиденциальность видимой: используйте понятный и понятный язык для объяснения практики сбора и использования данных.
- 3) Предоставьте обратную связь и контроль: предоставьте пользователям обратную связь по их настройкам конфиденциальности и простые в использовании элементы управления для их настройки.
- 4) Тестируйте и совершенствуйте: постоянно тестируйте и совершенствуйте подсказки, чтобы убедиться, что они эффективны в продвижении решений, благоприятных для конфиденциальности.
- 5) Проведение пользовательских исследований: проведение углубленных пользовательских исследований для сбора данных об их поведении, предпочтениях и мотивах, что позволит разработать эффективные методы подталкивания.
- 6) Разработка прототипов подталкиваний: создание и тестирование прототипов подталкиваний, совершенствование их конструкции и эффективности с помощью итеративного тестирования и обратной связи.
- 7) Оцените влияние подталкиваний: проведите тщательную оценку влияния подталкиваний на поведение пользователей, включая их эффективность в продвижении вариантов, благоприятных для конфиденциальности, и их возможные непреднамеренные последствия.



8) Усовершенствуйте структуру: постоянно совершенствуйте и обновляйте структуру на основе новых результатов исследований, гарантируя, что она останется актуальной и эффективной для продвижения решений, благоприятных для конфиденциальности.

Мы провели исследование для проверки эффективности нашей структуры. Мы разработали мобильное приложение, которое использовало подталкивания, чтобы побудить пользователей уделять первостепенное внимание своей конфиденциальности. Приложение использовало комбинацию визуальных подсказок, механизмов обратной связи и социальных норм, чтобы подталкивать пользователей к выбору, благоприятному для конфиденциальности. Наши результаты показали, что пользователи, которые получали подталкивания, с большей вероятностью уделяли первостепенное внимание своей конфиденциальности, чем те, кто этого не делал.

Результаты опроса были следующими:

- Возраст: среднее = 32,5, SD = 10,2
- Род занятий: 60% работающие специалисты, 20% студенты, 10% пенсионеры, 10% другие
- Образование: 50% степень бакалавра, 20% степень магистра, 15% докторская степень, 15% другое
- Использование мобильного приложения: 80% ежедневно, 15% несколько раз в неделю, 5% примерно раз в неделю
- 75% респондентов сообщили, что испытывают сильную или некоторую обеспокоенность по поводу сбора и использования их персональных данных мобильными приложениями.
- 80% респондентов сообщили, что для них очень или в некоторой степени важно, чтобы мобильные приложения защищали их персональные данные.
- 60% респондентов сообщили, что не очень уверены или совсем не уверены в том, что мобильные приложения защитят их персональные данные.
- 70% респондентов сообщили, что они с большей вероятностью будут использовать мобильное приложение, которое предоставляет четкую и прозрачную информацию о методах сбора и использования данных.



- 65% респондентов сообщили, что они с большей вероятностью будут использовать мобильное приложение, которое предоставляет обратную связь об их действиях по обмену данными.

- 75% респондентов сообщили, что они с большей вероятностью будут использовать мобильное приложение, позволяющее им контролировать настройки обмена данными.

**Выводимая статистика:**

- Тест хи-квадрат выявил значимую связь между уровнем обеспокоенности респондентов сбором данных и вероятностью использования ими мобильного приложения, предоставляющего четкую и прозрачную информацию о методах сбора и использования данных ( $\chi^2 = 12,45, p < 0,01$ ).

- Логистический регрессионный анализ показал, что респонденты, которые сообщили о сильной или некоторой обеспокоенности сбором данных, с большей вероятностью использовали мобильное приложение, которое предоставляло обратную связь об их деятельности по обмену данными ( $OR = 2,15, p < 0,05$ ).

- С помощью t-теста была выявлена значительная разница в уверенности респондентов в способности мобильных приложений защищать их персональные данные между теми, кто сообщил, что очень или немного обеспокоен сбором данных, и теми, кто сообщил, что не очень или совсем не обеспокоен ( $t = 2,56, p < 0,05$ ).

Заключение: В этой статье демонстрируется потенциал поведенческой экономики для информирования о разработке более эффективных решений РbD. Понимая психологические, социальные и эмоциональные факторы, которые влияют на принятие решений пользователем, дизайнеры могут создавать более ориентированные на пользователя проекты, которые ставят конфиденциальность пользователя на первое место. Наша структура обеспечивает отправную точку для интеграции поведенческой экономики в РbD, а наше исследование демонстрирует эффективность этого подхода.

**Литература:**

1) Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.

2) Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием



машинного обучения //Интеллектуальные технологии на транспорте. – 2018. – №. 3 (15). – С. 47-54.

3) Богомаз М. Э., Михайлова Л. А., Поляничева А. В. ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IP-ТЕЛЕФОНИИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 170-172.

4) Гельфанд А. М. Способы выбора стежоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262.

5) Свидетельство о государственной регистрации программы для ЭВМ № 2020664289 Российская Федерация. Программа обеспечения системы компьютерного зрения на основе библиотеки OpenCV : № 2020663625 : заявл. 03.11.2020 : опубл. 11.11.2020 / И. Е. Пестов, А. М. Гельфанд, Н. Н. Лансере, И. И. Фадеев ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». – EDN PKSCLB.



Александров Константин Игоревич

Студент 5 курс, факультет КБ

Институт телекоммуникаций им. проф. М.А. Бонч-Бруевича Россия

**ASSESSITS : ИНТЕГРАЦИЯ ПРОЦЕДУРНЫХ РЕКОМЕНДАЦИЙ И  
ПРАКТИЧЕСКИХ ПОКАЗАТЕЛЕЙ ОЦЕНКИ ДЛЯ ОЦЕНКИ  
ОРГАНИЗАЦИОННЫХ ИТ-РИСКОВ И РИСКОВ КИБЕРБЕЗОПАСНОСТИ**

Аннотация: В современном цифровом ландшафте надежные методы оценки рисков в области информационных технологий (ИТ) имеют важное значение для защиты систем, цифровой связи и данных. В этой статье представлен « AssessITS », действенный метод, разработанный для предоставления организациям всесторонних рекомендаций по проведению оценок рисков в области ИТ и кибербезопасности. Широко опираясь на NIST 800-30 Rev 1, COBIT 5 и ISO 31000, « AssessITS » устраняет разрыв между теоретическими стандартами высокого уровня и практическими проблемами внедрения. В статье излагается пошаговая методология, которую организации могут просто принять для систематического выявления, анализа и снижения рисков в области ИТ. Упрощая сложные принципы до действенных процедур, эта структура предоставляет специалистам инструменты, необходимые для самостоятельного выполнения оценок рисков, без чрезмерной зависимости от внешних поставщиков. Руководящие принципы разработаны так, чтобы быть простыми, интегрируя практические метрики оценки, которые позволяют точно количественно оценить стоимость активов, уровни угроз, уязвимости и воздействие на конфиденциальность, целостность и доступность. Такой подход гарантирует, что процесс оценки рисков будет не только всеобъемлющим, но и доступным, что позволит лицам, принимающим решения, внедрять эффективные стратегии снижения рисков, адаптированные к их уникальным операционным контекстам. Цель « AssessITS » — дать организациям возможность повысить уровень своей ИТ-безопасности с помощью практических, действенных рекомендаций, основанных на международно признанных стандартах.

*Ключевые слова : кибербезопасность , информационная безопасность , оценка риска , оценка риска , снижение риска , уровень угрозы , оценка уязвимости, СПбГУТ им. Проф. Бонч- Бруевича.*



*Keywords: Cybersecurity, Information security, Risk assessment, Risk assessment, Risk reduction, Threat level, Vulnerability assessment, SPbSUT im. Prof. Bonch-Bruевич.*

В то время, когда информационные технологии (ИТ) являются основой практически всех бизнес-операций, эффективное управление рисками, связанными с ИТ, имеет решающее значение для поддержания организационной стабильности и безопасности. Эффективное управление ИТ-рисками имеет первостепенное значение. Однако исследования показывают, что традиционные структуры по-прежнему сталкиваются с проблемами в надлежащем решении сложной природы ИТ-угроз. ИТ-риски включают неопределенности, возникающие из-за недостаточной информации об угрозах, передовых технологиях и внутренних организационных уязвимостях, среди прочих проблем. В этой статье представлен целостный подход к оценке рисков, называемый «*AssessITS*». Он сочетает пошаговые инструкции с реалистичными метриками оценки для повышения эффективности методов управления ИТ-рисками. Этот метод не только стремится обнаруживать и снижать риски, но и готовит организации к адаптации к различным рабочим ситуациям, тем самым укрепляя их способность противостоять будущим перебоям в работе ИТ и кибербезопасности.

Исследование вводит новшества, объединяя теоретические рамки, такие как NIST 800-30 Rev.1, COBIT 5 и ISO 31000, в практическую, настраиваемую методологию. В то время как каждая из этих рамок рассматривает конкретные подходы к оценке рисков, «*AssessITS*» оптимизирует их в единый подход. Эта интеграция упрощает сложные оценки ИТ-рисков, предоставляя четкие, выполнимые шаги и метрики, которые облегчают их внедрение в различных отраслях и организационных размерах. По сравнению с существующими стандартами, которые часто требуют существенной интерпретации, «*AssessITS*» предлагает более прямой путь от теории к практической реализации. 3. Однако эти стандарты были выбраны для этого исследования из-за их мирового признания в управлении и руководстве ИТ-рисками. NIST 800-30 фокусируется на процессах оценки рисков, COBIT 5 на руководстве и управлении ИТ, а ISO 31000 предоставляет комплексные рекомендации по управлению рисками. Вместе они создают сбалансированную и надежную основу, подходящую для оценки рисков ИТ и кибербезопасности.

Расширение цифровой инфраструктуры требует повышенного внимания к взаимодействию между фреймворками управления ИТ и динамическими настройками



рисков. Хотя такие фреймворки, как COBIT, предоставляют стандартизированные методологии, которые имеют решающее значение для согласования ИТ-операций с бизнес-целями, им по-прежнему не хватает способности адаптироваться и реагировать в режиме реального времени на новые риски. Более того, динамичная и постоянно меняющаяся природа рисков кибербезопасности требует большего, чем фиксированные модели; она требует фреймворка, который не только предсказывает возможные слабые стороны, но и включает в себя процедуры постоянного обучения и корректировки. Исследования показывают, что существует значительная разница в эффективности текущих методов управления рисками, особенно когда речь идет о работе со сложностями организаций и технологий. «*AssessITS*» решает эти трудности, предлагая универсальный, основанный на данных подход, который связывает теоретические концепции с практическим выполнением, тем самым укрепляя организационную устойчивость к ИТ-угрозам и угрозам кибербезопасности. Целью исследования является разбиение руководств высокого уровня на конкретные, управляемые задачи. Для организаций всех размеров и отраслей оно предоставляет метрики оценки и процедурные руководства, которые упрощают оценку рисков, обеспечивая ясность в реализации и гарантируя, что даже небольшие организации смогут эффективно применять эту матрицу. Эта стратегия предлагает потенциал не только для упрощения операций по оценке рисков, но и для улучшения стратегической интеграции оценки ИТ-рисков с общими целями компании.

Оценка рисков является неотъемлемой частью комплексного процесса управления рисками и необходима для эффективного управления информационной безопасностью в бизнесе. Этот процесс подразумевает методический анализ возможных рисков для деятельности, активов и персонала организации, а также обнаружение слабых мест как из внутренних, так и из внешних источников. Процесс включает оценку негативных последствий, которые могут возникнуть, если эти угрозы воспользуются известными слабыми местами, и определение вероятности таких событий. Это позволяет организации принимать обоснованные решения о том, как реагировать на риски в соответствии с ее общей стратегией управления рисками. Подход подчеркивает важность оценки рисков для сохранения безопасности организации и включает ее в общую структуру управления рисками, поощряя проактивный подход к устранению потенциальных угроз безопасности. Комплексная структура управления рисками начинается с определения фрейма риска, который устанавливает основу путем описания фона среды и определения методологии для последующих выборов, связанных с рисками. Фаза оценки риска включает в себя



выявление и оценку угроз и уязвимостей. Этот шаг имеет решающее значение, поскольку он предоставляет информацию для процесса принятия решений путем расчета возможного воздействия и вероятности неблагоприятных событий. После этого инициируется компонент реагирования на риски, в котором бизнес формулирует и внедряет решения, специально разработанные для снижения воздействия выявленных рисков, придерживаясь при этом заранее определенной толерантности к риску. Реализация стратегии упреждающего реагирования имеет решающее значение для обеспечения организационной устойчивости к потенциальным угрозам. Наконец, этап мониторинга рисков гарантирует эффективность усилий по управлению рисками с течением времени, адаптируясь к изменениям в операционной среде и согласуя с общими целями организации и предварительными условиями соответствия. Постоянное наблюдение имеет решающее значение для постоянного улучшения тактики управления рисками и обеспечения долгосрочного благополучия безопасности организации.

Эффективное управление рисками в динамической области кибербезопасности опирается на сложные и гибкие подходы к оценке рисков. Выделенная многокритериальная структура принятия решений демонстрирует сложный способ оценки рисков кибербезопасности путем всесторонней оценки нескольких компонентов риска. Этот подход систематически измеряет угрозы, уязвимости и потенциальные последствия, объединяя их с помощью аналитического подхода к принятию решений для успешной расстановки приоритетов в методах управления рисками. Оценивая риски по различным измерениям, включая физические, информационные и социокогнитивные аспекты, он представляет собой сложные взаимосвязи, типичные для современных киберсистем.

Основное преимущество подхода заключается в его способности не только обнаруживать и изучать стационарные риски, но и адаптироваться к постоянно меняющейся природе проблем кибербезопасности. Он помогает лицам, принимающим решения, предлагая четкую и организованную процедуру, которая соответствует корпоративным целям и технологическим критериям, что позволяет стратегически реагировать на киберугрозы. Включение многокритериального анализа в оценки рисков кибербезопасности является существенным улучшением для общего управления рисками. Такая интеграция обеспечивает более полное понимание угроз и способствует созданию более надежных систем кибербезопасности.

Целостная стратегия, объединяющая качественные и количественные подходы, необходима при оценке идей оценки рисков для различных отраслей, таких как



авиационные системы и средний бизнес. Значимость сложных, многогранных методов оценки рисков при обнаружении, анализе и снижении киберугроз подчеркивается в нескольких отраслях. Крайне важно, чтобы эти структуры оценки рисков были разработаны так, чтобы быть гибкими, позволяя включать новые меры и технологии безопасности. Эта гибкость необходима для борьбы с новыми опасностями, такими как криптоджекинг и бесфайловые программы-вымогатели, которые могут измениться и остаться незамеченными. Существующие структуры оценки рисков необходимо срочно расширить, чтобы учесть изменения, которые технология блокчейн привносит в ИТ-инфраструктуры в различных секторах, включая здравоохранение, банковское дело, оборонные модели и академические круги. Чтобы гарантировать эффективную безопасность и интеграцию на всех платформах, эти структуры должны включать как традиционные ИТ-установки, так и отличительные особенности технологии блокчейн. Такой комплексный подход способствует внедрению успешных методов комплексного управления ИТ-рисками, повышая проектирование надежных решений по кибербезопасности, адаптированных к уникальным промышленным проблемам.

В сфере ИТ и кибербезопасности в организациях специалисты-практики обычно следуют структурированному и комплексному подходу при построении основы оценки рисков.

Этот подход включает четыре ключевых шага: подготовка к оценке, проведение оценки, сообщение результатов и поддержание результатов оценки с течением времени. Процесс оценки начинается с обзора, который устанавливает фундаментальную основу для эффективного взаимодействия с риск-средой. Подготовительные мероприятия имеют решающее значение для обеспечения всеобъемлющего состояния готовности. За этими мероприятиями следует систематическое выполнение оценки, целью которой является сбор и анализ соответствующих данных о рисках. Следовательно, в этом разделе будут рассмотрены методы эффективного сообщения и распространения результатов оценки рисков для обеспечения того, чтобы все заинтересованные стороны были хорошо информированы и активно участвовали. Наконец, в разделе подчеркивается важность последовательного поддержания результатов для точного представления изменяющейся риск-среды. Это достигается за счет использования комплексных таблиц рисков и шкал оценки, которые помогают стандартизировать процесс оценки. Исследователи описывают каждую фазу с помощью конкретных задач, предоставляя организациям дополнительные рекомендации по эффективному выполнению оценок рисков, иллюстрируя основные шаги



и выделяя соответствующие задачи.

Одним из наиболее важных шагов в процессе оценки риска является третий шаг, который включает эффективное сообщение результатов и распространение информации, связанной с риском, по всей организации. Этот шаг гарантирует, что лица, принимающие решения, имеют необходимую информацию для принятия обоснованных решений о рисках.

Сотрудники службы безопасности должны выполнить две конкретные задачи: во-первых, четко и всесторонне сообщить результаты оценки риска, а во-вторых, распространить информацию, собранную в ходе оценки, для поддержки других важных мероприятий по управлению рисками. Важно предоставить подробное и всестороннее описание этого сообщения. Это включает представление результатов и методологий таким образом, чтобы они были понятны и понятны всем заинтересованным сторонам. В сфере устройств Интернета медицинских вещей (IoMT) для оценщика риска крайне важно распознавать сложную природу ландшафта риска, на который в первую очередь влияет разнообразный спектр используемых технологий. Следовательно, становится необходимым адаптировать стратегии коммуникации для эффективного удовлетворения различных уровней понимания среди различных заинтересованных сторон. Важно обеспечить, чтобы информация, которой обмениваются, была не только понятной, но и действенной, способствуя принятию эффективных решений по управлению рисками в различных отделах и командах. Благодаря стратегической интеграции структурированных задач коммуникации и обмена информацией организации имеют потенциал для значительного повышения прозрачности и эффективности своих процессов управления рисками.

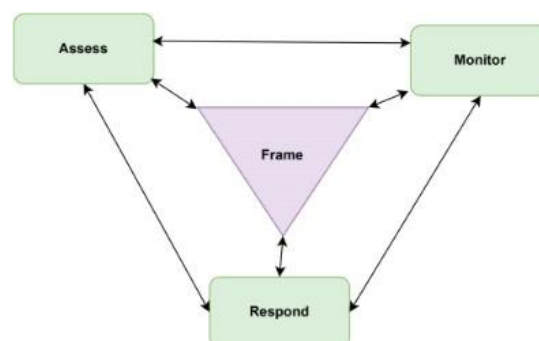
Принятие проактивной и хорошо информированной стратегии имеет решающее значение для исследователей для эффективного управления и снижения потенциальных рисков в постоянно меняющейся среде рисков.

Поддержание оценки рисков должно быть непрерывным процессом для каждой организации, поскольку это позволяет им эффективно корректировать свои стратегии управления рисками в соответствии с постоянно меняющимся ландшафтом угроз, технологическими достижениями и развивающимися методами исследований. Важно проводить периодические обзоры и обновления, чтобы гарантировать, что оценки остаются актуальными и точно отражают самые последние проблемы безопасности и конфиденциальности. Организационная практика проведения оценок рисков каждые



шесть месяцев демонстрирует систематический подход к упреждающему выявлению и устранению потенциальных уязвимостей. Регулярные обновления оценки и исправления выявленных рисков с использованием новых данных должны практиковаться в плановом порядке. Кроме того, организациям необходимо проверять эффективность реализованных стратегий снижения рисков. Этот процесс помогает адаптироваться к изменениям в информационных системах организации и средах, в которых они функционируют, гарантируя постоянное соответствие и соответствие толерантности организации к риску. Благодаря постоянному поддержанию актуальной оценки рисков организации могут получать ценную информацию, которая позволит им принимать обоснованные решения. Эти решения не только улучшают общую безопасность организаций, но и обеспечивают соответствие нормативным требованиям. Кроме того, путем проактивного управления рисками безопасности и конфиденциальности организации могут повысить свою долгосрочную операционную устойчивость и способствовать своему стратегическому успеху.

Концепции оценки риска, науки и управления рисками всегда сложны, и они становятся все сложнее с каждым днем просто из-за разрушительных методов коммуникации, подозрительности властей и растущих требований к участию общественности в процессе принятия решений. Согласно NIST, управление рисками - это непрерывный процесс, который управляет рисками в различных областях организации, таких как операции, активы или отдельные лица, где оценка риска является дополнительным компонентом управления рисками. Существует четыре компонента процесса управления рисками: (I) определение риска, (II) оценка риска, (III) реагирование на риск и (IV) мониторинг риска.



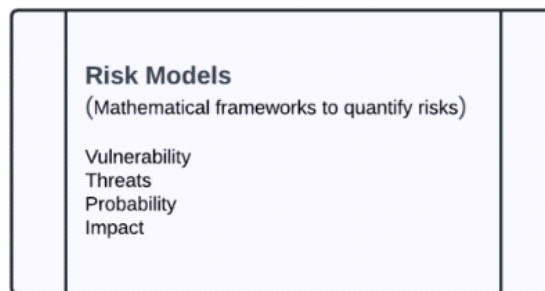
С быстрым ростом информационных и коммуникационных технологий



неопределенность и угрозы следуют очень значительной восходящей тенденции. Вероятные потери, связанные с этой неопределенностью и угрозой, известны как риск. Риск - это измерение возможных потерь, которые могут возникнуть в будущем из-за нежелательных обстоятельств. Оценка вероятных потерь и вероятность возникновения нежелательных обстоятельств - две неотъемлемые части риска. Термин риск является неотъемлемой частью каждой бизнес-организации. Нет ни одной организации или отдела, которые были бы свободны от риска. Идея рисков различается от отдела к отделу и от организации к организации. В случае информационных и коммуникационных технологий денежные или репутационные потери, связанные с утечками данных, потерей данных и нарушениями безопасности, являются некоторыми примерами риска.

Для проведения надлежащей оценки рисков крайне важно следовать надежным методологиям оценки рисков, которые тесно связаны со структурой бизнеса. Методологии оценки рисков основаны на статистическом или вероятностном анализе, который оценивает влияние неблагоприятных обстоятельств на организацию. Оценка рисков, модель риска, подход к оценке и подход к анализу являются некоторыми существенными частями методологий оценки рисков.

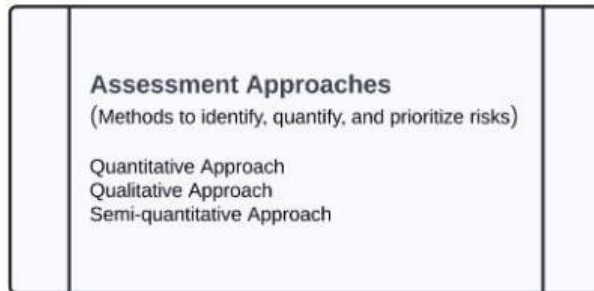
- 1) Модели риска: Как правило, модель риска представляет собой



математическое представление факторов, которые учитываются при оценке риска. Модель риска также пытается определить взаимосвязь и влияние факторов. Фактор риска варьируется от организации к организации. Некоторые из важнейших факторов риска, которые являются общими почти для каждой организации, — это уязвимость, угроза, вероятность, влияние и предрасполагающее состояние, как показано на рисунке. Модели риска могут сильно отличаться от организации к организации. Модель риска для финансов не похожа на модель бухгалтерского учета. Аналогично, модели риска не совсем одинаковы в каждом ИТ-отделе. Раданлиев разработал надежную модель для измерения максимально возможных потерь за определенный период времени,



сосредоточившись на влиянии Интернета вещей на экономику, тогда как Кандасами разработал модель риска, ориентированную на Интернет вещей, с использованием фреймворка, известного как CORAS, который основан на UML. Даже если оба они сосредоточены на оценке риска Интернета вещей, их модели риска различаются из-за различий в организационной структуре и целях.



2) Подходы к оценке: С ростом сложности подрывных инноваций организациям становится чрезвычайно сложно следовать единому подходу к оценке рисков. В современном мире не существует идеального подхода к оценке рисков. Организациям необходимо выбрать один подход из набора альтернатив, который наилучшим образом соответствует их целям и организационной культуре. NIST предлагает три надежных подхода к оценке рисков, которые известны как 1) количественный подход, 2) качественный подход и 3) полуколичественный подход, как показано на рисунке .

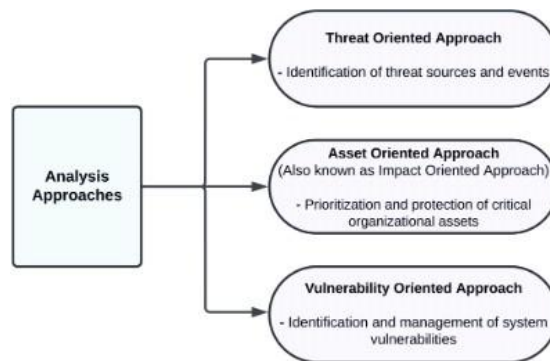
3) Подходы к анализу: Аналитическая часть по сути является ядром оценки риска. Результат оценки риска в значительной степени зависит от качества анализа риска. NIST предлагает три подхода к анализу риска: а) подход, ориентированный на угрозы, б) подход, ориентированный на активы, и с) подход, ориентированный на уязвимости. Все эти подходы отличаются друг от друга из-за факторов изменчивости, таких как начальный аспект оценки риска, степень детализации и способ обработки угроз.

Первым приоритетом подхода, ориентированного на угрозы, является определение источников угроз и событий угроз. Этот подход также сохраняет свое внимание на разработке сценариев угроз наряду с определением уязвимости контекста угрозы. Кроме того, этот подход определяет эффект враждебных угроз на основе намерения антагониста. Подход, ориентированный на активы или подход, ориентированный на воздействие, определяет чувствительные активы и последствия рассматриваемой области, тогда как подход, ориентированный на уязвимости, начинается с определения набора недостатков



или ограничений общих процессов. Он также подробно определяет события угроз.

Каждый из подходов рассматривает одни и те же факторы риска и, следовательно, охватывает схожие типы оценочных мероприятий, но в разных порядках, как показано на рисунке. Организации также могут использовать дополнительные подходы к анализу строгости, такие как анализ на основе графов, который отличается от трех подходов, предложенных NIST.



Чтобы определить, какие активы или услуги следует оценивать в контексте управления рисками, начните с создания тщательного перечня всех материальных и нематериальных активов, а также связанных с ними процессов и услуг. Вещи в этом списке должны быть классифицированы на основе их типов, таких как оборудование, программное обеспечение или данные. После категоризации ранжируйте каждый элемент на основе его важности для бизнес-операций и его общей критичности. Такая расстановка приоритетов облегчает оценку их восприимчивости и возможных последствий угроз безопасности. В конечном итоге выберите наиболее важные активы, процессы или услуги для проведения тщательной оценки, уделяя особое внимание тем, которые, если их подорвать, будут представлять наивысший уровень угроз для бизнеса. Этот методический прием гарантирует целенаправленную и эффективную процедуру оценки рисков.

Чтобы определить стоимость активов внутри организации, крайне важно привлечь важные субъекты, такие как Комитет по организационной ИТ-безопасности, Руководящий комитет ИТ и Комитет по управлению рисками. Начните с определения ключевых заинтересованных сторон из этих комитетов для участия в процессе оценки. После этого должны быть установлены критерии оценки стоимости чего-либо, которые должны охватывать такие факторы, как финансовые последствия, правовые последствия,



операционные эффекты и ущерб репутации. Организуйте обзорные семинары или встречи с этими комитетами для анализа и оценки стоимости каждого актива в соответствии с определенными критериями. Используйте механизм оценки, например шкалу от 1 до 5, для присвоения рейтингов стоимости каждому активу, которые будут отражать объединенный вклад комитетов, как показано в Таблице 1. В конечном счете, крайне важно записывать и документировать эти значения и проводить регулярные оценки, чтобы гарантировать их точность и применимость к текущим требованиям компании.

Этот кооперативный метод гарантирует тщательную и сбалансированную оценку стоимости активов, что необходимо для эффективного снижения рисков. Ниже приведены некоторые общие ИТ-активы, процессы и услуги, которые следует учитывать, хотя этот список не ограничивается этими примерами.

Актив/Услуга	Стоимость актива/услуги (1 - 5)
Основное программное обеспечение	Это значение должно быть определено владельцем системы и CIO, а затем предложено и одобрено одним из комитетов по управлению рисками или безопасности организации. Значение должно учитывать как материальные, так и нематериальные аспекты актива, услуги или процесса.
Первичная база данных	
Сетевая инфраструктура	
Облачные службы хранения данных	
Центр обработки данных	
Решения по обеспечению непрерывности бизнеса (DR/Far DR)	
Интегрированные операции по обеспечению безопасности	
Системы обработки платежей	
Конечное устройство	
Веб-сервер	
Файловый сервер	
Сервер электронной почты	
Системы управления взаимоотношениями с клиентами (CRM)	

Чтобы определить и оценить уровень риска для каждого актива, начните с составления списка потенциальных угроз с помощью таких методов, как сеансы знаний, анализ прошлых данных, моделирование угроз, наблюдения из внутренних и внешних аудитов, анализ журналов инцидентов, оценки уязвимости, тестирование на проникновение и консультации с отраслевыми отчетами, среди прочих подходов. Расширьте этот список, включив информацию с платформ анализа угроз и отраслевых баз данных. Оцените серьезность этих угроз, рассмотрев такие элементы, как денежные потери, сбои в работе, правовые последствия и ущерб репутации, используя такие фреймворки, как NIST SP 800- 30 или ISO/IEC 27005 и подходящее программное обеспечение для оценки рисков.

Присвойте числовое значение каждой угрозе на основе заранее определенной



системы оценок (например, шкалы от 1 до 5), чтобы точно измерить степень ее воздействия, как показано в Таблице 2. Запишите эти открытия в консолидированную базу данных, используя такие технологии, как программное обеспечение для управления рисками или Excel. Последовательно оценивать и пересматривать список потенциальных угроз и их уровни серьезности, чтобы быть в курсе изменений в ландшафте угроз и среде, в которой находятся активы. Это можно сделать с помощью запланированных обзоров и автоматических предупреждений от платформ анализа угроз, гарантируя, что реестр рисков остается актуальным. Эта комплексная стратегия гарантирует, что оценки рисков являются исчерпывающими, а меры по смягчению последствий нацелены с большой эффективностью.

Уровень угрозы	
Рейтинг угрозы	Влияние на бизнес
1	Незначительный
2	Незначительный
3	Умеренный
4	Главный
5	Катастрофический

Для оценки уязвимостей и их влияния на триаду Конфиденциальность, Целостность и Доступность (CIA) инициируется выявление уязвимостей с использованием таких методов, как сканеры уязвимостей, тестирование на проникновение и аудит безопасности. Это должно быть дополнено изучением системных журналов, конфигураций и отчетов о прошлых инцидентах. Затем оцените возможное влияние каждой уязвимости на конфиденциальность, целостность и доступность организации. Это включает в себя выявление возможности несанкционированного раскрытия информации, манипулирования данными или нарушения работы служб. Оцените влияние каждой уязвимости на триаду CIA, используя заранее определенную шкалу от 1 (незначительное влияние) до 5 (наивысшее влияние), чтобы оценить серьезность, как показано в Таблице 3. Запишите эти результаты в централизованном репозитории, используя программное обеспечение или инструменты управления рисками, такие как Excel или Google Sheets, для хорошо организованной документации. Регулярно оценивайте и пересматривайте эту оценку, чтобы учитывать изменения в среде угроз, настройках системы и протоколах безопасности, гарантируя постоянную защиту и готовность к реагированию на инциденты.



Уровень уязвимости	
(Влияние VA определено с учетом существующих уязвимостей, мер по их устранению и воздействия на ЦРУ)	
Рейтинг уязвимости	Влияние на бизнес
1	Незначительный
2	Низкий или минимальный
3	Середина
4	Высокий
5	Самый высокий

Определение мер по устранению уязвимостей, влияющих на триаду

«Конфиденциальность, целостность и доступность» (CIA), запущенных путем разработки целевых стратегий устранения, таких как исправления программного обеспечения, обновления конфигурации и улучшения политики. Расставьте приоритеты этих действий на основе серьезности и риска для критических функций организации, оценив необходимые ресурсы, такие как бюджет, персонал и время для осуществимости.

Реализуйте эти меры в порядке приоритета и постоянно отслеживайте их эффективность в смягчении уязвимостей. Ведите подробную документацию всех мер по устранению и результатов и регулярно отчитывайтесь перед заинтересованными сторонами, чтобы адаптироваться к меняющимся угрозам и организационным изменениям. Этот структурированный подход обеспечивает постоянное соответствие целям безопасности и управления рисками. Чтобы точно оценить эффективность оценки уязвимости (VA) после исправления, начните с повторной оценки восприимчивости каждого актива к угрозам, учитывая обновленные факторы, такие как местоположение, доступность и усиленные меры безопасности. Повторно оцените влияние уязвимостей на конфиденциальность, целостность и доступность, используя шкалу от 0 (никакого воздействия) до 4 (критическое воздействие), наряду с подверженностью актива угрозам, которая теперь оценивается от 1 (незначительный риск) до 5 (наивысший риск), чтобы отразить улучшения исправления, как показано в Таблице 4. Объедините эти обновленные показатели, чтобы сформировать всеобъемлющий рейтинг уязвимости, который фиксирует остаточные риски после исправления. Документируйте и организуйте эти результаты в программном обеспечении для управления рисками или электронных таблицах, обеспечивая регулярные обзоры для поддержания точности в соответствии с меняющимся ландшафтом угроз. Эта структурированная повторная оценка имеет решающее значение для измерения эффективности исправления и определения приоритетов будущих усилий по обеспечению безопасности на основе серьезности оставшихся рисков и подверженности актива. Исследование проводилось на основе



концепций NIST и ISO и позволило разработать практическую версию общего рейтинга уязвимости после устранения неполадок.

Идентификатор уязвимости	Актив затронут	Уровень воздействия	Влияние на конфиденциальность (0-4)	Влияние на целостность (0-4)	Влияние на доступность (0-4)	Общий рейтинг уязвимости (1-5)
ВУЛ 1	Веб-сервер	Высокий	4	3	0	Общая оценка по показателям конфиденциальности, целостности и доступности (CIA) должна устанавливаться путем объединения отдельных рейтингов CIA, отражающих эффективность мер по устранению нарушений, текущие потребности в обеспечении безопасности и, что наиболее важно, уровень допустимого риска, установленный организацией.
ВУЛ 2	Сервер базы данных	Середина	2	4	4	
ВУЛ 3	Ноутбук сотрудника	Низкий	3	2	3	

Чтобы оценить риск, начните с определения уровня угрозы по шкале от 1 до 5, где 1 означает низкую угрозу, а 5 означает значительную угрозу. Используйте эти оценки для вычисления степени опасности, используя следующее уравнение: Значение угрозы = Уровень угрозы + Уровень уязвимости. После выполнения расчетов сохраните эти значения угроз в централизованном репозитории, чтобы гарантировать, что все данные методически документированы и легко доступны для непрерывного управления рисками. Чтобы оценить вероятность атак, приступайте к сбору исторических данных из предыдущих отчетов об инцидентах, каналов разведки угроз и отраслевой статистики, чтобы оценить частоту сопоставимых угроз. Оцените существующую среду угроз, используя платформы разведки угроз и рекомендации по безопасности, чтобы получить полное представление о потенциальных опасностях. Оцените различные критерии, включая уровень уязвимости активов, эффективность текущих мер безопасности и возможности возможных злоумышленников. Используйте предоставленные оценки для назначения оценок вероятности с использованием predetermined шкалы от 1 (указывающей на редкость) до 5 (указывающей на высокую вероятность), как показано в

Таблице 5. Запишите эти оценки в централизованную базу данных и внедрите регулярный процесс оценки и пересмотра оценок, чтобы гарантировать их точность и отражение любых изменений в ландшафте угроз.



Вероятность	
Рейтинг	Возможность возникновения
1	Очень маловероятно
2	Маловероятно
3	Возможный
4	Вероятный
5	Очень вероятно

Мы рассчитываем рейтинг воздействия риска путем умножения стоимости актива, стоимости угрозы и вероятности по формуле  $\text{Рейтинг воздействия риска} = \text{Стоимость актива} * \text{Стоимость угрозы} * \text{Вероятность}$ . Хотя эти задачи представлены последовательно для ясности, важно отметить, что в действительности некоторая итерация среди задач является как существенной, так и ожидаемой. В зависимости от конкретной цели оценки риска бизнес может обнаружить, что перераспределение обязанностей может быть выгодным. Оценки риска должны соответствовать заявленной цели, области действия, предположениям и ограничениям, установленным субъектом, который их инициирует, независимо от любых внесенных изменений. Критерии, изложенные ниже, предоставлены командой « AssessITS », однако они могут различаться в разных организациях в зависимости от их индивидуальных уровней толерантности к риску. Структура уровня критичности риска адаптирует принципы категоризации рисков из руководства NIST 800-30. Хотя NIST использует качественный и полуколичественный подход, наша модель вводит подробную систему оценок (от 1 до 250) для назначения уровней риска, таких как Низкий, Средний, Высокий и Критический, на основе потенциального воздействия и вероятности угроз, как показано в Таблице 6. Это позволяет проводить более детальную оценку рисков, помогая организациям эффективнее расставлять приоритеты в своих ответных мерах.

Уровень критичности риска	
Рейтинг и оценка	Возможность возникновения
1 (от 1 до 45)	Низкий
2 (46-99)	Середина
3 (от 100 до 199)	Высокий
4 (от 200 до 250)	Критический

Ниже представлен подробный пошаговый предполагаемый сценарий, тщательно разработанный для полного соответствия представленной выше Матрице оценки рисков с учетом установленных стандартов оценки рисков.

- 1) Идентификация актива и владельца
  - Актив/Услуга: Веб-сервер, Владелец: ИТ-отдел



- 2) Стоимость активов (AV)
  - 4 — Критически важно для бизнес-операций, размещения важных приложений.
- 3) Выявление угроз
  - Включает общие угрозы кибербезопасности, которые могут повлиять на веб-сервер, такие как несанкционированный доступ, кража данных и сбои в работе служб.
- 4) Уровень угрозы (TV)
  - 4 (Основной) — Рассмотрение наихудшего сценария для критически важного актива, такого как веб-сервер.
- 5) Оценка уязвимости
  - Выявленные уязвимости включают недостаточную защиту брандмауэра и устаревшее серверное программное обеспечение.
- 6) Меры по исправлению положения
  - Никаких мер по исправлению ситуации не было реализовано, поскольку компания не готова приобрести новый брандмауэр. Кроме того, обновление программного обеспечения сервера нецелесообразно, поскольку текущая веб-служба, запущенная на этом сервере, несовместима с новой версией.
- 7) Влияние на ЦРУ
  - Влияние на ЦРУ:  $C - 4, I - 4, A - 4$
- 8) Уровень уязвимости
  - 5 (наивысший), учитывая выявленные уязвимости, отсутствие мер по их устранению и их влияние на ЦРУ
- 9) Расчет величины угрозы (TV)
  - $TV = \text{Уровень угрозы} + \text{Уровень уязвимости} = 4 + 5 = 9$
- 10) Вероятность угрозы (LH)
  - Вероятность оценивается как 4 (Вероятно), поскольку уровни как угрозы, так и уязвимости высоки, что указывает на то, что веб-сервер подвергается значительному риску кибератаки.
- 11) Расчет рейтинга воздействия риска (RI)
  - $RI = AV \times TV \times LH = 4 \times 9 \times 4 = 144$
- 12) Уровень критичности риска
  - Высокий (144), уровень критичности риска классифицируется как высокий. Значения от 100 до 199 классифицируются как высокие согласно критериям « AssessITS »



Закключение: Это исследование проиллюстрировало эффективность стратегии « *AssessITS* »

» в преодолении разрыва между теоретическими принципами оценки рисков и их фактической реализацией в областях ИТ и кибербезопасности. « *AssessITS* » повышает эффективность оценки рисков и укрепляет способность предприятий противостоять киберугрозам, используя признанные стандарты, такие как NIST, COBIT и ISO. В будущем « *AssessITS* » будет хорошо позиционирован для адаптации и минимизации возникающих рисков, что сделает его решающим в постоянно меняющейся области цифровой безопасности. Постоянное развитие и совершенствование этого подхода будет иметь важное значение для прогнозирования и решения меняющихся проблем безопасности, гарантируя его значимость для стратегии оценки рисков.

#### Литература:

1. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных
2. //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Шариков П. И., Красов А. В., Штеренберг С. И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов //Т-Comm- Телекоммуникации и Транспорт. – 2017. – Т. 11. – №. 3. – С. 66-70.
4. Сахаров Д. В. и др. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе Ipv6 //Защита информации. Инсайд. – 2020. –
5. №. 1. – С. 51-57.
6. Красов А. В., Шариков П. И. Методика защиты байт-кода Java-программы от декомпиляции и хищения исходного кода злоумышленником //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2017. – №. 1. – С. 47-50.
7. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.



## Юридические науки



## DIGITAL LAW: NAVIGATING THE LEGAL LANDSCAPE OF THE DIGITAL AGE

Annotation: In the rapidly evolving digital age, the intersection of technology and law has given rise to a new and dynamic field known as digital law. This area encompasses a wide range of legal issues that arise from the use of digital technologies, including data protection, cybersecurity, intellectual property, and e-commerce. As our reliance on digital platforms and services continues to grow, understanding digital law has become increasingly important for individuals, businesses, and governments alike.

*Keywords: digital law, legal landscape.*

*Ключевые слова: цифровое право, правовой ландшафт.*

### The Scope of Digital Law

Digital law covers a broad spectrum of legal issues that emerge from the digital transformation of society. Some of the key areas include:

#### 1. Data Protection and Privacy

With the increasing amount of personal data being collected and stored online, data protection has become a critical concern. Laws such as the General Data Protection Regulation (GDPR) in Europe aim to protect individuals' personal data and ensure that it is handled responsibly .

#### 2. Cybersecurity

As cyber threats become more sophisticated, the need for robust cybersecurity measures has never been greater. Digital law addresses the legal frameworks and standards that organizations must adhere to in order to protect their digital assets and prevent cyber attacks .

#### 3. Intellectual Property

The digital age has brought new challenges to intellectual property rights. Digital law deals with issues related to copyright, trademarks, and patents in the digital realm, ensuring that creators and innovators are protected .

#### 4. E-commerce

With the rise of online marketplaces, digital law governs the legal aspects of e-commerce, including consumer protection, contract law, and payment systems .



## 5. Digital Contracts and Electronic Signatures

Digital law also covers the legal validity of digital contracts and electronic signatures, ensuring that they are enforceable and secure .

### **The Importance of Digital Law**

The importance of digital law cannot be overstated. It plays a crucial role in protecting individuals' rights, ensuring fair competition, and fostering innovation. By providing a legal framework for the digital landscape, digital law helps to build trust and confidence in digital technologies and services.

For businesses, understanding digital law is essential for compliance and risk management. Failure to adhere to digital laws can result in significant legal and financial consequences, including **fin**es, **lawsuits**, and **damage to reputation** .

### **Challenges in Digital Law**

Despite its importance, digital law faces several challenges. The rapid pace of technological change often outpaces the development of legal frameworks, leading to gaps and uncertainties in the law. Additionally, the global nature of the digital landscape presents jurisdictional challenges, as laws may vary significantly from one country to another .

Another challenge is the need for balance between protecting individuals' rights and fostering innovation. Overly restrictive laws can stifle innovation, while lax regulations can leave individuals vulnerable to exploitation and abuse .

### **The Future of Digital Law**

As technology continues to evolve, so too will digital law. Emerging technologies such as **artificial intelligence**, **blockchain**, and **the Internet of Things (IoT)** will present new legal challenges and opportunities. Digital law will need to adapt and evolve to address these developments, ensuring that the legal framework keeps pace with technological advancements .

### **Case Study: The Role of Digital Evidence in Legal Proceedings**

Digital evidence plays a crucial role in modern legal proceedings, providing valuable insights and proof in various cases. One notable example is the case of Michelle Carter, who was convicted of involuntary manslaughter in 2017. The prosecution relied heavily on digital evidence, including text messages and phone calls, to prove that Carter had encouraged her boyfriend, Conrad Roy III, to commit suicide.

This case highlighted the significance of digital evidence in legal investigations and underscored the need for robust digital evidence management practices .



In conclusion, digital law is a vital and dynamic field that plays a crucial role in shaping the digital landscape. By providing a legal framework for the use of digital technologies, digital law helps to protect individuals' rights, ensure fair competition, and foster innovation. As technology continues to evolve, the importance of digital law will only grow, making it an essential area of study and practice in the digital age .

**References:**

1. Wikipedia. (2025). Digital rights. [https://en.wikipedia.org/wiki/Digital\\_rights](https://en.wikipedia.org/wiki/Digital_rights)
2. Miller Digital Citizenship. (2017). What is digital law? <https://millerdigitalcitizenship.weebly.com/digital-law.html>
3. Digital Law Journal. The purpose of the Digital Law Journal. [https://www.digitallawjournal.org/jour?locale=en\\_US](https://www.digitallawjournal.org/jour?locale=en_US)
4. JP Defense. (2024). What is digital law. <https://jpdefense.com/what-is-digital-law/>
5. Linley James Solicitors. Digital law.
6. Cornell Law School. (1995). Digital Law: Some Speculations on the Future of Legal Information Technology. <https://www.law.cornell.edu/papers/fut95fnl.htm>
7. Precise Digital. (2020). 4 Cases Solved With Digital Evidence.



## THE ROLE OF LAWYERS IN THE GLOBAL FINANCIAL MARKET

Annotation: In the intricate and ever-evolving landscape of the global financial market, lawyers play a pivotal role in ensuring compliance, facilitating transactions, and managing risks. Their expertise is crucial in navigating the complex regulatory environment and addressing the legal challenges that arise in cross-border financial activities. This article explores the significance of lawyers in the global financial market and presents a case study to illustrate their impact.

*Keywords: lawyers, global financial market.*

*Ключевые слова: юристы, мировой финансовый рынок.*

### **The Multifaceted Role of Lawyers.**

#### **1. Regulatory Compliance.**

Lawyers specializing in financial markets are instrumental in helping clients comply with the myriad of regulations that govern financial activities. They stay abreast of changes in laws and regulatory frameworks, such as those implemented by the *Securities and Exchange Commission (SEC) in the U.S. or the Financial Conduct Authority (FCA) in the UK*. Their advice ensures that financial institutions and corporations operate within the bounds of the law, mitigating the risk of legal penalties and reputational damage.

#### **2. Transactional Support.**

Lawyers are integral to the structuring and execution of complex financial transactions. They draft and negotiate contracts, conduct due diligence, and provide legal opinions on the enforceability of agreements. Their involvement is essential in mergers and acquisitions, initial public offerings (IPOs), and other significant corporate transactions. For instance, *Jones Day's Financial Markets Practice* has facilitated over \$6 trillion in financing transactions over the past five years, demonstrating the scale and complexity of deals that lawyers handle .

#### **3. Risk Management.**

In the financial sector, risk management is paramount. Lawyers identify and assess legal risks associated with financial products, investments, and market activities. They develop strategies to mitigate these risks, including the implementation of robust governance structures



and internal controls. Their role is particularly critical in managing risks related to financial derivatives, securitization, and other complex financial instruments.

#### **4. Dispute Resolution.**

Despite careful planning, disputes can arise in the financial market. Lawyers represent clients in litigation, arbitration, and other dispute resolution processes. They advocate for their clients' interests, seeking to resolve disputes efficiently and effectively. Their expertise in financial law and regulation is invaluable in navigating the complexities of financial disputes.

#### **5. Innovation and Adaptation.**

The financial market is continually evolving, driven by technological advancements and innovative financial products. Lawyers must adapt to these changes and provide legal guidance on emerging issues, such as the regulation of cryptocurrencies and the legal implications of fintech. For example, the Master's Programme 'Lawyer on the Global Financial Market' at HSE University focuses on innovation in law and finance, equipping lawyers with the skills to address these challenges .

#### **Case Study: Hertz Global Holdings.**

##### **Background:**

*Hertz Global Holdings*, a well-known car rental company, faced significant financial challenges in the early 2020s. The company had accumulated substantial debt and was exploring options to restructure its capital and improve its financial stability

##### **Legal Strategy:**

Lawyers played a crucial role in advising Hertz on its capital restructuring options. They assessed the feasibility of issuing new equity to rebalance the company's capital structure and reduce its debt burden. The legal team also evaluated the potential market response to a rights offering, considering the historical reactions to similar moves by established companies.

##### **Outcome:**

In 2019, Hertz successfully held a rights offering and restructured some of its debt. The legal advice and strategic planning contributed to the company's efforts to achieve sustainable profitability. The case of Hertz Global Holdings illustrates the importance of legal expertise in navigating complex financial restructuring and capital management processes .

##### **Conclusion.**

Lawyers are indispensable in the global financial market, providing essential legal support and strategic advice to financial institutions and corporations. Their role in ensuring regulatory compliance, facilitating transactions, managing risks, resolving disputes, and adapting



to innovation is crucial for the stability and growth of the financial sector. The case of Hertz Global Holdings underscores the significance of legal expertise in achieving successful financial outcomes. As the financial market continues to evolve, the demand for skilled lawyers who can navigate its complexities will remain high.

**References:**

- Yale School of Management. Finance Case Studies.  
<https://som.yale.edu/centers/international-center-for-finance/icf-case-studies>
- HSE University. Master's Programme 'Lawyer on the Global Financial Market'.  
<https://www.hse.ru/en/ma/finlaw/>
- Jones Day. Financial Markets Practice.  
<https://www.jonesday.com/en/practices/financial-markets?tab=overview>



Зинин Николай Викторович

Магистрант

Частное учреждение высшего образования «Московская академия предпринимательства»

## **ЗАКОННАЯ НЕУСТОЙКА: ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ**

Аннотация: В настоящей статье проводится анализ теоретических основ и практического применения законной неустойки как правового инструмента гражданского законодательства. Рассмотрена её роль в системе гражданско-правовых обязательств, а также выполнен анализ вопросов, связанных с её применением и реализацией на практике. В работе также освещаются проблемные аспекты, возникающие в ходе практического использования института законной неустойки.

*Ключевые слова: законная неустойка, гражданское право, обязательства, ответственность, юридическая практика.*

*Keywords: legal penalty, civil law, obligations, liability, legal practice.*

Действующее гражданское законодательство различает законную и договорную неустойки. В соответствии со ст. 332 Гражданского кодекса РФ (далее – ГК РФ ) под законной неустойкой понимается определенная законом денежная сумма, которую должник обязан уплатить кредитору в случае неисполнения или ненадлежащего исполнения обязательства, в частности, в случае просрочки исполнения.

Несмотря на то, что указанный институт был известен еще в дореволюционном отечественном праве, сколько-нибудь значимой доктринальной проработке до настоящего времени он так и не подвергался. Подобное игнорирование института законной неустойки выглядело нормальным в условиях советской системы гражданского права, в рамках которой обозначенный механизм получил весьма широкое распространение и необходимость существования которого не вызывала сомнений.

Подавляющее большинство современных научных исследований, посвященных неустойке, как правило, либо полностью сосредоточены на анализе ее договорного типа, либо ограничиваются формальным указанием на существующую классификацию в зависимости от оснований ее возникновения [1].



Вместе с тем при таком подходе упускается из виду, пожалуй, самое главное. А именно тот факт, что основания возникновения законной и договорной неустойки отражают лишь следствие, но не причины, лежащие в основе указанного деления. Указанный институт в современных условиях развития рыночной экономики представляет собой прежде всего механизм законодательного ограничения свободы договора.

С этой точки зрения принципиально важным становится поиск ответов на вопросы об эффективности законной неустойки, о целесообразности ее дальнейшего сохранения, о пределах использования положений о законной неустойке, о соотношении данной правовой категории со схожими механизмами ограничения свободы договора. Анализ действующего законодательства показывает, что на сегодняшний день отсутствует четкое понимание того, в каком направлении должен развиваться обозначенный институт, какими критериями следует руководствоваться при его установлении применительно к той или иной группе гражданско-правовых отношений.

Таким образом, при исследовании законной неустойки в современных условиях на первый план должен выйти его анализ в качестве механизма ограничения свободы договора. Рассмотрение данного правового явления в таком срезе позволит ответить на поставленные выше вопросы, а также сформулировать ряд предложений, направленных на оптимизацию действующего законодательства в области законных неустоек.

В последнее время наблюдается тенденция к увеличению количества судебных дел, связанных с взысканием договорной неустойки, доля таких дел составляет 25-30% от общего числа гражданских дел, рассматриваемых судами. Размер неустойки обычно колеблется от 0,1% до 1% от суммы задолженности за каждый день просрочки. В крупных коммерческих контрактах размер неустойки может достигать 20-30% от общей суммы договора, что существенно влияет на оценку рисков сторонами.

Законная неустойка является существенным институтом гражданского права, играющим ключевую роль в обеспечении исполнения обязательств сторонами. Законная неустойка представляет собой предварительно оговорённую денежную сумму, которую одна сторона договора обязана уплатить другой стороне в случае нарушения условий договора, а именно, при невыполнении обязательств или их ненадлежащем исполнении. С теоретической точки зрения, законная неустойка выполняет профилактическую, компенсационную и санкционную функции, что делает ее незаменимым механизмом регулирования гражданско-правовых отношений [2].



В Российской Федерации правовое регулирование законной неустойки осуществляется Гражданским кодексом Российской Федерации. Данный кодекс устанавливает порядок применения неустойки, в том числе:

- Статьей 330 предусматривается возможность для сторон договора самостоятельно определять размер неустойки.
- Статья 333 ГК РФ предусматривает механизмы корректировки размера неустойки в случае ее признания судом чрезмерной [3].

Сравнительный анализ законодательств различных государств выявляет существенные различия в подходах к регулированию договорных неустоек. В некоторых юрисдикциях, таких как страны общего права (США, Великобритания, Канада и др.), наблюдается более строгий контроль за размерами неустоек, что ограничивает свободу сторон в определении условий их применения. В отличие от этого, российское законодательство предоставляет сторонам больший простор для самостоятельного установления параметров неустойки [2,4].

В контексте углубления международной экономической интеграции и глобализации, приобретает особую актуальность анализ применения законной неустойки в Российской Федерации. Необходимо исследовать существующие практические сложности в этой области и разработать эффективные меры по их преодолению.

На практике реализация норм о законной неустойке сопряжена с рядом вызовов. Во-первых, нередко наблюдается неопределенность в отношении размера неустойки. Многие контрагенты устанавливают завышенные значения, что может повлечь злоупотребления и противоречить принципу разумности. Во-вторых, кредиторы иногда сталкиваются с трудностями при доказывании фактических убытков, что создаёт препятствия для применения компенсационных мер. В-третьих, законодательство требует обязательного согласования размеров законной неустойки в контракте, что может осложнить процесс заключения соглашений. Кроме того, чрезвычайно важно, чтобы положения о договорной неустойке были сформулированы максимально ясно и конкретно. Необходимо указать не только величину неустойки, но и процедуру ее расчета, а также условия, при которых она подлежит применению. Нечеткость формулировок может стать причиной разногласий.

Одной из актуальных проблем является недостаток единой судебной практики по применению норм о законной неустойке. Несогласованность в подходах различных судов к оценке одних и тех же факторов приводит к правовой непредсказуемости. В ряде



случаев стороны могут злоупотреблять правом, устанавливая чрезмерно высокие размеры неустойки или используя её как инструмент давления на контрагента. Это создаёт препятствия как для заключения соглашений, так и для эффективного судебного разбирательства.

Законодательно установленная неустойка играет значительную роль в гражданско-правовых отношениях. Правильное её понимание и применение существенно упрощает ведение коммерческой деятельности и минимизирует количество судебных разбирательств [4]. Для совершенствования практики применения неустойки необходимо не только неукоснительное соблюдение законодательных норм, но и развитие правоприменительной практики с учётом обеспечения законных интересов всех участников.

Институт законной неустойки играет важную роль в гражданском праве, обеспечивая исполнение обязательств и выполняя профилактическую, компенсационную и санкционную функции. Однако, несмотря на свою значимость, этот институт до сих пор остается недостаточно исследованным и вызывает ряд практических трудностей, включая неопределенность в размерах неустойки, сложность доказательства убытков и отсутствие единообразия в судебной практике. В условиях рыночной экономики законная неустойка рассматривается как механизм ограничения свободы договора, что требует дополнительного анализа и поиска решений для повышения эффективности и справедливости ее применения.

#### **Литература:**

- 1 Богдан В. В. Практика применения норм о взыскании неустойки в свете нового Постановления Пленума Верховного Суда РФ «О рассмотрении судами гражданских дел по спорам о защите прав потребителей» // Право и экономика. 2020. № 3. С. 76 – 79.
- 2 Белов А.А. Договорная неустойка: проблемы правоприменения // Экономика и социум. 2022. № 11-2 (102). С. 318–322;
- 3 Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 №51-ФЗ (ред. от 08.08.2024);
- 4 Крупенич Е.А. Правовое регулирование неустойки // Скиф. Вопросы студенческой науки. 2020. №5. С. 253-257;
- 5 Колдина Ю.Р. Неустойка как способ защиты прав имущественного интереса субъекта // Вопросы российской юстиции. 2021. № 11. С. 209-214;



Сокор Александр Анатольевич

Магистрант

Негосударственное образовательное частное учреждение  
высшего образования «Московский финансово-промышленный  
университет «Синергия»

## НАСЛЕДОВАНИЕ ПО ЗАКОНУ И ЗАВЕЩАНИЮ: ТЕОРИЯ И ПРАКТИКА

**Аннотация:** Наследственное право занимает ключевое место в системе правопреемства, позволяя передавать материальные и нематериальные блага от умерших к наследникам. Автор анализирует существующие проблемы, связанные с интерпретацией и применением норм о наследовании по закону и по завещанию. Исследование подчеркивает значимость наследственного права для стабильности гражданского оборота и предлагает пути совершенствования правовой базы.

*Ключевые слова:* наследственное право, наследование по закону, наследование по завещанию, юридическая практика, исполнитель завещания.

*Keywords:* inheritance law, inheritance by law, inheritance by will, legal practice, executor of the will.

Наследственное право является фундаментальной составляющей юридической системы, обеспечивающей процесс правопреемства от умершего к другим лицам. Данный процесс включает передачу как материальных, так и нематериальных благ, накопленных человеком в течение его жизни. Значимость наследственного права обусловлена его ролью в регулировании социальных и экономических отношений, а также в обеспечении стабильности гражданского оборота. Наследование может осуществляться по двум основным основаниям: по закону и по завещанию. Наследование по закону применяется в случаях, когда завещание отсутствует или признано недействительным. В этом случае наследство распределяется между наследниками в порядке, установленном законодательством, обычно по степени родства. Наследование по завещанию предоставляет наследодателю самостоятельно определить круг наследников и условия распределения наследства, что отражает принцип свободы завещания. Однако,



несмотря на детальное правовое регулирование, на практике возникают различные трудности [1].

Изучение наследования не теряет своей актуальности в современной юридической науке и практике.

Существенное значение данного правового института подчеркивается не только количеством судебных дел, связанных с переходом права собственности после смерти владельца имущества, но и наличием дискуссионных, открытых к доктринальному решению вопросов, связанных с эффективным регулированием данной сферы правоотношений. Согласно действующему законодательству Российской Федерации, каждый гражданин имеет право владеть имуществом. Общее правило имеет определённые исключения, закреплённые в федеральных законах, указывающих на объекты, которые не могут быть объектами частной собственности (особо охраняемые природные территории, объекты культурного наследия).

Также строго регламентированы механизмы перехода права собственности посредством передачи и принятия наследства.

Прежде всего, право на наследование, возникающее и реализуемое в случае смерти гражданина, гарантируется Конституцией Российской Федерации. Также в пункте 2 статьи 218 Гражданского кодекса Российской Федерации (далее - ГК РФ) определяется, что право собственности на имущество умершего переходит к его наследникам в соответствии с завещанием или, при его отсутствии - на основании закона. Такой подход определяет значимость завещательных распоряжений, которые позволяют гражданам самостоятельно определять судьбу своего имущества после смерти. В целом, это способствует более осознанному и ответственному отношению к распределению личных активов, предотвращению возможных конфликтов и споров между наследниками.

Рост рыночных отношений сопровождается увеличением объектов гражданского оборота, в частности, недвижимости, что оказывает непосредственное влияние на динамику совершаемых сделок. Соответственно, увеличивается и число наследственных дел, так как с ростом объема приватизированного имущества усиливается потребность граждан в юридическом оформлении прав на наследуемое имущество. Соответственно, не теряет своей востребованности задача разработки эффективного правового регулирования процедур наследования. В действующем законодательстве он представлен в разделе V «Наследственное право» части третьей Гражданского кодекса РФ. Вступив в действие с 1



марта 2002 года, она до сих пор служит надёжной основой регламентации отношений, связанных с передачей прав и обязанностей умершего лица его правопреемникам.

В целом, следует утверждать, что законодательное закрепление наследственного права в указанной части ГК РФ ознаменовало собой начало нового этапа. Детализация порядка наследования на уровне федерального кодифицированного закона позволяет разрешать наследственные споры с учётом особенностей различных ситуаций. Кроме того, подчёркивается значимость нотариального участия в процессе наследования, что усиливает защиту прав наследников и минимизирует риски нарушения их прав в результате недобросовестных действий третьих лиц [2].

Значимость выявления особенностей правового регулирования наследования по закону обусловлена необходимостью теоретического осмысления и конструктивного критического анализа особенностей текущего правового регулирования наследования по закону, практического решения проблем, возникающих на пути реализации гражданами их прав наследования[3].

Между тем, для описания наследования по закону в ГК РФ предусмотрено всего десять статей (ст. 1141-1151). Для регулирования наследования по завещанию – отведено двадцать две статьи (ст. 1118-1140 ГК РФ). Такая ситуация объясняется желанием законодателя предоставить гражданам максимальную свободу в вопросах передачи их имущества посредством индивидуально оформленного завещания. У каждого собственника имеется возможность указать, кто именно должен стать его наследником. Завещание предоставляет возможность детально распределить своё имущество с учетом личных отношений и предпочтений, что делает этот процесс высоко индивидуализированным и важным инструментом личного и семейного планирования.

Напротив, наследование по закону регулирует более общие случаи, когда завещание отсутствует. Оно устанавливает стандартную процедуру распределения имущества, основанную на степени родства, что обеспечивает защиту прав всех потенциальных наследников в равной степени.

Такая схема предусматривает простоту и предсказуемость в регулировании наследственных отношений и является гарантом того, что имущество умершего будет распределено справедливо согласно установленным законом приоритетам.

Одной из фундаментальных концепций наследственного права Российской Федерации является принцип свободы завещания. Он подразумевает, что каждый гражданин имеет право самостоятельно определять судьбу своего имущества после своей



смерти. Однако важно понимать, что данная свобода не является абсолютной и может подвергаться определённым ограничениям, которые законодательство предусматривает с целью защиты интересов других лиц или общества в целом. В частности, закон защищает права несовершеннолетних детей умершего, предоставляя им обязательную долю в наследстве, независимо от содержания завещания[4].

Законодательство Российской Федерации устанавливает различные способы и формы завещательных распоряжений, целью которых является обеспечение доступности процедуры составления завещаний и предоставление правообладателям практической возможности определить условия передачи своего имущества после смерти.

Однако детальный анализ действующего законодательства показывает, что, несмотря на значительные усилия по совершенствованию правовой базы, существующая система не лишена определённых недостатков, которые могут ограничивать эффективность наследственных передач. В частности, возможности совершения закрытого завещания ограничены определённым кругом лиц. Закрытое завещание, представляющее собой документ, содержание которого не разглашается до смерти завещателя и который обеспечивает высокий уровень конфиденциальности, доступно не для всех категорий наследодателей, что может стать препятствием для тех, кто стремится сохранить приватность своих последних волеизъявлений. Такие ограничения, хотя и обусловлены необходимостью защиты прав всех заинтересованных сторон, в некоторых случаях могут препятствовать полному раскрытию воли наследодателя, особенно в сложных семейных или финансовых обстоятельствах.

Остается актуальным и требует дополнительной правовой проработки вопрос регулирования процедуры составления закрытого завещания. Согласно действующему законодательству, оно представляет собой документ, который завещатель должен написать и подписать лично. Такой подход предполагает полную дееспособность и физическую способность лица к самостоятельному выполнению этих действий. Однако значительное количество граждан из-за различных обстоятельств не может совершить такие действия самостоятельно. Лица, находящиеся на длительном лечении в медицинских учреждениях, военнослужащие или граждане, находящиеся в экстремальных условиях, длительных рейсах на судах в открытом море, сталкиваются с ограничениями в возможности составления закрытого завещания. Обозначенная правовая коллизия ограничивает их право на самостоятельное распоряжение собственным имуществом после смерти [5].



Требуют своего решения вопросы, связанные с изменением и отменой завещаний. Дополнительные сложности возникают при реализации норм об исполнении завещания. Нуждаются в уточнении правила, касающиеся выполнения последней воли завещателя. С учетом вышеизложенного, необходима комплексная реформа законодательства, касающегося наследственного права, особенно в части формы и порядка составления завещаний, а также норм, регулирующих их изменение и исполнение.

При этом, важно понимать, что разделение на наследование по закону и по завещанию не влечет второстепенности одного из порядка по сравнению с другим. Оба они составляют единую систему, основанную на общих правовых и нравственных принципах, и взаимно дополняют друг друга, обеспечивая полноту правовой защиты интересов всех потенциальных правопреемников. Различие между ними заключается прежде всего в юридических механизмах возникновения прав и обязанностей у наследников, что предопределяет разные подходы к оформлению наследства [6].

Наследственное право строго регулируется законодательством, которое определяет порядок и условия приобретения наследства, включая сроки для принятия наследства, порядок его оформления и отказа от наследства.

Переосмысление идеологии наследственного права в современной России связано с переходом к новым экономическим и социальным реалиям. В новом понимании наследственное право начинает играть важнейшую роль в поддержании стабильности и предсказуемости правоотношений, помогает в управлении переходом имущественных прав и интересов от одного поколения к другому, обеспечивая справедливое и законное распределение ресурсов. Основными принципами наследственных правоотношений являются принцип универсального правопреемства, очередность призвания наследников, принцип свободы завещания, обеспечение необходимых интересов и прав наследников, свобода выбора у наследников, призванных к наследованию, защита наследства от чьего-либо незаконного посягательства [7].

Современная реформа наследственного права в Российской Федерации основывается на принципах частноправовой регламентации.

Во-первых, экономическое измерение реформы проявляется в расширении круга объектов, которые могут быть предметом наследования. Такое изменение способствует интеграции различных видов активов в экономический оборот и упрощает процесс смены правообладателей, что является значительным шагом к обеспечению более эффективного распределения ресурсов в обществе. Теперь в качестве объектов наследственного



правопреемства могут выступать не только традиционные формы имущества, но и ценные бумаги, доли в бизнесе, цифровые активы и даже права на интеллектуальную собственность.

Во-вторых, в рамках реформирования утверждается приоритет наследования по завещанию перед наследованием по закону. Данное изменение подчеркивает важность волеизъявления умершего и его право самостоятельно распоряжаться своим имуществом после смерти. Завещание становится не просто инструментом передачи имущества, но и выражением личных взглядов, предпочтений и даже культурных и нравственных ценностей наследодателя.

Третьей важной особенностью реформы является расширение свободы завещания и усиление гарантий его реального исполнения. Современное законодательство предоставляет наследодателям более широкие возможности точного определения условий наследования, включая создание фондов, завещательных распоряжений на случай смерти и других сложных юридических конструкций. В целом, это способствует большей юридической защищенности потенциальных наследников и минимизации конфликтов, возникающих из-за неопределенности прав на наследство.

Осуществленное исследование позволило сформулировать следующие выводы и предложения, указало на необходимость внесения следующих изменений в ГК РФ с целью совершенствования института наследования по закону и завещанию:

1. Предлагаем законодательно закрепить понятие завещания под которым следует понимать одностороннюю сделку, содержащую распоряжения наследодателя, то есть гражданина, обладающего в момент его совершения дееспособностью в полном объеме, в отношении принадлежащего ему имущества на случай его смерти, выполненную в предусмотренной законом форме и создающую права и обязанности после открытия наследства

2. Предлагаем под принятием наследства понимать этап правопреемства, который начинается с момента смерти наследодателя и предполагает совершение юридических действий для перехода имущества к наследникам. Российское гражданское законодательство устанавливает требования к порядку, срокам оформления наследственных прав.

3. Предлагаем под отказом от наследства понимать одностороннюю сделку (как выражение воли одного субъекта - наследника) по отречению от принятия полагающейся ему в целом либо доли имущества, или имущественного права (наследственной массы).



Отказ от наследства должен соответствовать принципам безусловности, необратимости и универсальности.

4. Предлагаем изложить в новой редакции статью 1156 «Переход права на наследство (наследственная трансмиссия)» ГК РФ:

«1. Если наследник, призванный к наследованию по завещанию или по закону, умер после открытия наследства, не успев его принять в установленный срок, право на принятие причитавшегося ему наследства переходит к его наследникам по закону, а если все наследственное имущество было завещано - к его наследникам по завещанию (наследственная трансмиссия). Право на принятие наследства в порядке наследственной трансмиссии не входит в состав наследства, открывшегося после смерти такого наследника.

1.1. Если наследник, призванный к наследованию по закону в течение срока, установленного для принятия наследства (ст. 1154) не принял наследства, то право на принятие наследства переходит к наследникам следующей очереди. Данное право они могут осуществить в течение шести месяцев со дня истечения срока для принятия наследства наследником предыдущей очереди. Данное право приобретают наследники каждой последующей очереди.

1.2. Если наследник, принявший наследство, не осуществляет пользования наследством, то наследник последующей очереди вправе обратиться в суд для признания за ним права на наследование, если будет доказано, что он нуждается в имуществе, входящем в состав наследства.

2. Право на принятие наследства, принадлежавшее умершему наследнику, может быть осуществлено его наследниками на общих основаниях. Если оставшаяся после смерти наследника часть срока, установленного для принятия наследства, составляет менее трех месяцев, она увеличивается до трех месяцев. По истечении срока, установленного для принятия наследства, наследники умершего наследника могут быть признаны судом принявшими наследство в соответствии со статьей 1155 настоящего Кодекса, если суд найдет уважительными причины пропуска ими этого срока.

3. Право наследника принять часть наследства в качестве обязательной доли (статья 1149) не переходит к его наследникам».

4. Предлагаем п. 2 ст. 1131 ГК РФ изложить в следующей редакции: «Признание завещания недействительным возможно после открытия наследства, как в случаи с оспоримыми, так и в случаи с ничтожными завещаниями, по иску лица, чьи законные



интересы нарушены данным завещанием». Таким образом, ничтожным можно признать завещание как в случае, когда это прямо указано в гражданском кодексе, так и в тех случаях, когда в нем не соблюдаются правила к порядку его оформления и составления. Очень часто это относится к завещаниям, которые составлены не нотариусом, а другими лицами, перечень которых содержится в статье 1127 ГК РФ.

5. Предлагаем внести завещание гражданина, находящегося в других странах, удостоверенные в посольствах РФ консулами в список завещаний, приравненных к нотариально удостоверенным, поскольку консулы обладают достаточной квалификацией и являются представителями подданных РФ.

6. Предлагаем внести в статью 1131 ГК РФ норму, которая увеличит количество душеприказчиков или же право перехода на наследников по завещанию.

7. Предлагаем внести корректировки в пункт 2 статьи 1126 ГК РФ. Изменить формулировку «закрытое завещание должно быть собственноручно написано и подписано завещателем» - на «закрытое завещание должно быть составлено на бланке нотариуса и подписано завещателем». Такой подход поможет правильно составить завещание и не допустить двусмысленности при его токовании.

Подводя итог вышеизложенного можем отметить, что результаты исследования не только подтвердили актуальность и значимость проблематики наследования по закону и по завещанию, но и предложили конкретные направления для дальнейшего совершенствования правового регулирования.

#### **Литература:**

1. Алхастова М.В. Понятие и значение наследования по завещанию // EurasiaScience. - Москва: Общество с ограниченной ответственностью «Актуальность.РФ», 2023. - С. 422-423.
2. Горбунов З.Н. Деятельность нотариуса при определении объема наследственной массы и принятии мер по охране наследства: теория и практика применения // Нотариальный вестник. - 2023. - № 9. - С. 42-50.
3. Гориславец Т.М. Особенности института наследования по завещанию // Студенческий. - 2023. - № 34-4(246). - С. 9-13.
4. Казанцева А.Е. Теория наследственного и причастных к нему правоотношений по гражданскому праву Российской Федерации: автореф. дис. ...д-ра юрид. наук. - Томск, 2015. - 46 с.



5. Кубинец Т.В. Гражданско-правовое положение субъектов наследования // Конституция Российской Федерации как гарант прав и свобод человека и гражданина. - Ростов-на-Дону: Ростовский государственный университет путей сообщения, 2021. - С. 45-48.

6. Лукьянов М.А. Общая характеристика наследования по завещанию и по закону // Актуальные проблемы общества, экономики и права в контексте глобальных вызовов. - Санкт-Петербург: Печатный цех, 2023. - С. 426-434.

7. Туник Р.П. Реализация принципа гуманизма // Правовая система и современное государство: проблемы, тенденции и перспективы развития. - 2020. - С. 84-88.



## Экономические науки



Ишимов Денис Вадимович

Диджитал маркетолог, продюсер онлайн школ, ИП

## ЭФФЕКТИВНЫЕ МЕТОДЫ СОЗДАНИЯ АВТОВОРОНОК В DIGITAL-МАРКЕТИНГЕ

Аннотация: В статье рассматриваются современные и результативные методы создания автоворонок с позиций цифрового маркетинга, которые выступают в качестве весьма значимого инструмента автоматизации взаимодействия с аудиторией, повышения конверсии. Актуальность данной темы обуславливается явным усилением роли digital-технологий в маркетинговой практике, потребностью в оптимизации затрат, ужесточением конкуренции на рынке. Цель исследования заключается в систематизации и проведении анализа ключевых методов построения изучаемых воронок, выявлении факторов, влияющих на их действенность, формулировке рекомендаций относительно их оптимизации. В работе отмечаются противоречия в научной литературе: одни авторы акцентируют внимание на технологических инновациях (применение нейросетей, чат-ботов), другие же делают упор на контентную составляющую, нюансы персонализации. Сделан вывод о том, что успешное создание автоворонок требует комплексного подхода, представленного, прежде всего, интеграцией современных технологий, анализом поведения аудитории, налаживанием каждого этапа контакта с клиентами. Авторские предложения аргументированы через призму интеграции с CRM-системами, более активного использования чат-ботов, геймификации процессов (подразумевается обращение к игровым механикам), обучающих материалов. Изложенное в статье будет полезно маркетологам, предпринимателям, аналитикам, а также исследователям, которые занимаются изучением инструментов digital-маркетинга.

*Ключевые слова:* автоворонка, автоматизация, аналитика, аудитория, взаимодействие, конверсия, маркетинг, персонализация, технологии.

*Keywords:* autorock, automation, analytics, audience, interaction, conversion, marketing, personalization, technology.



## Введение

В современной цифровой среде автоворонки стали одним из ключевых инструментов для автоматизации процессов привлечения, вовлечения, а также конверсии клиентов. Рассматриваемые системы предоставляют возможность минимизировать затраты времени и ресурсной базы, обеспечивая непрерывное взаимодействие с целевой аудиторией. Одновременно с этим по мере роста конкуренции на digital-платформах возрастает необходимость разработки более точных, адаптивных методов формирования автоворонок, способных удовлетворить изменяющиеся запросы со стороны пользователей.

Проблема данного исследования заключается в том, что многие маркетологи сталкиваются с трудностями при проектировании анализируемых в статье воронок, включая:

- недостаточную персонализацию;
- сложность анализа этапов взаимодействия;
- достаточно низкую конверсию на отдельных уровнях.

С учетом этого уместно подчеркнуть, что без грамотного подхода к построению таких систем нереально добиться устойчивых результатов, что делает вопрос разработки результативных методов актуальным для современной практики.

Итак, в нынешних условиях весьма значим анализ ключевых направлений создания автоворонок, изучение вариантов их оптимизации, выработка рекомендаций для повышения их действенности на фоне динамично развивающегося рынка.

## Материалы и методы

Исследования по обсуждаемой теме охватывают богатый спектр аспектов, в том числе, концептуальные наработки, технологические возможности, прикладные методы, специфические области применения.

Так, инновации в создании автоворонок рассматриваются в работах А.В. Ботиенко, А.А. Федориной [1], Е.А. Никуйко, Н.Е. Прошкина [5]. Пристальное внимание уделяется задействованию чат-ботов для автоматизации взаимодействия с клиентами, что помогает повысить результативность за счет оперативной обработки запросов. Также делается акцент на внедрении нейросетей, которые обеспечивают персонализацию сообщений, подстраивание контента под поведение пользователей в режиме «здесь и сейчас».

Практические методики создания автоворонок анализируются в публикациях С.А. Казаряна [2], Д. Пивкина [6], А.А. Умаргалеевой [8]. Предлагается использовать



продуктовые матрицы для интеграции в общий маркетинговый процесс компании; высвечивается значение персонализации. Помимо этого, демонстрируется описание пошагового процесса создания автоворонок «с нуля», фокусируясь на структуре ее этапов и оптимизации каждого из них. Также, дается характеристика специфике применения анализируемого инструментария в продвижении организаций (с обоснованием его роли в сокращении маркетинговых затрат).

Образовательные нюансы применительно к теме освещаются в трудах О.И. Матасовой, Д.В. Груне [4], К.А. Татарина [7], П.С. Шаманаева [10]. Указанные авторы своими изысканиями показывают, как автоворонки трансформируют процесс продаж соответствующих услуг, повышая вовлеченность студентов, упрощая взаимодействие с аудиторией. Ученые фокусируются на эффективности данного инструментария, рассматривают особенности его использования для онлайн-консультаций в массовом обучении. В дополнение к отмеченному, обсуждается значение воронок в сегменте открытых интернет-курсов.

Продвижение через социальные сети и цифровые платформы анализируется А.В. Цехомским и коллегами [9]. Исследование демонстрирует, как автоворонки возможно интегрировать в соцсети (с учетом специфики российского сегмента интернета), что содействует привлечению целевой аудитории, оптимизации ее пути к конверсии.

Сравнительный анализ сервисов для создания рассматриваемых в статье воронок представлен в публикации Д.М. Купцовой [3]. Автор описывает функциональные опции популярных платформ, оценивая их удобство использования, а также адаптивность под различные задачи предпринимательства.

Обзор материалов отражает разнообразие подходов к раскрытию темы — от технологических инноваций, применения нейросетей до образовательных, маркетинговых стратегий. Однако между авторами существуют разногласия. Некоторые исследователи делают акцент на автоматизации [1, 5], другие сосредоточены на контентной составляющей и человеческом факторе [2, 7]. Недостаточно проработанными остаются вопросы долгосрочной эффективности автоворонок, их адаптации под малый бизнес. Также требует большего внимания анализ рентабельности задействования различных платформ, инструментов.

Методы, используемые при раскрытии темы, — контент-анализ, сравнение, кейс-стади, обобщение.

### **Результаты и обсуждение**



Для начала целесообразно обратиться к раскрытию существенных характеристик автоворонки, специфике их структуры.

Так, они представляют собой систему автоматизированных действий, которые направлены на преобразование потенциальных клиентов в реальных покупателей [2, 4]. Их роль отражена в виде схемы на рисунке 1.

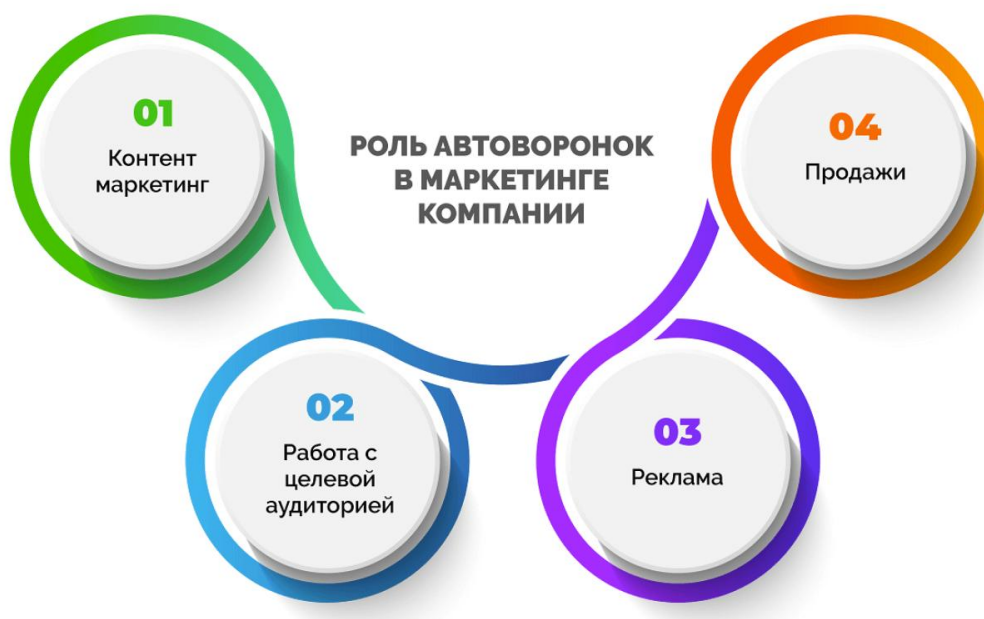


Рис. 1. Значение автоворонки в digital-маркетинге [6]

Fig. 1. The value of the autorocks in digital marketing [6]

Базовый принцип работы состоит в последовательном воздействии на целевую аудиторию, начиная от ее привлечения и завершая удержанием после совершения покупки.

Исторически концепция автоворонки восходит к классической модели продаж, предложенной еще в прошлом столетии. В ее основе была заложена идея этапности: привлечение внимания, формирование интереса, стимулирование желания, побуждение к действию. Впоследствии, с развитием технологий, это начало автоматизироваться. В 1960-1970-х годах, когда компании приступили к активному использованию базовых форм компьютерной обработки информации, появились первые попытки систематизировать взаимодействие с клиентами.

По мере развития интернета и электронной коммерции в 1990-х годах маркетологи начали деятельно применять рассылки и базы данных с целью таргетирования клиентов. Это явилось отправной точкой для формирования концепции автоматизации продаж.



Появление CRM-систем в начале 2000-х годов позволило управлять данными о клиентах более результативно, а переход на SaaS-модели в 2010-х годах открыл доступ к инструментам для создания автоворонки более широкому кругу пользователей.

Ключевым моментом в эволюции рассматриваемого в статье инструментария следует признать внедрение поведенческого таргетинга и триггерных механизмов [5, 8]. Эти разработки помогли настраивать воронки таким образом, чтобы каждая последующая коммуникация зависела от действий, которые клиент совершил на предыдущих этапах. Например, если пользователь не открыл письмо с предложением, система отправляет ему дополнительное напоминание либо изменяет контент очередного сообщения.

Современная концепция опирается на интеграцию аналитических платформ, искусственного интеллекта, технологий машинного обучения. Это предоставляет возможность как автоматизировать стандартные процессы, так и прогнозировать поведение клиентов, разрабатывать персонализированные маршруты взаимодействия, приспосабливать стратегию в режиме реального времени. Ввод характеризуемых подходов в практику сделал автоворонки важнейшим инструментом digital-маркетинга, обеспечивающим хозяйствующим субъектам гибкость, точность, масштабируемость привлечения и удержания пользователей.

Итак, концептуальная база автоворонки представляет собой синтез классических теорий продаж и современных решений, что позволяет маркетологам эффективно управлять контактами с аудиторией в условиях растущей конкуренции и стремительно меняющегося рынка.

Структура исследуемых воронок включает несколько элементов (рис. 2), каждый из которых выполняет свою функцию:



Рис. 2. Структурная характеристика авторонок  
(составлено автором на основе [1-3, 5, 9, 10])

Fig. 2. Structural characteristics of autorocks  
(compiled by the author on the basis of [1-3, 5, 9, 10])

Целесообразно подчеркнуть, что требуется максимально отчетливое понимание целевой аудитории, использование новейших технологий для анализа ее поведения.



Далее следует перейти к характеристике методов создания эффективной автоворонки.

Так, персонализация является базисом успеха в данной области, поскольку она помогает настроить взаимодействие под конкретного клиента. Это достигается через анализ поведения пользователя, его предпочтений, интересов. К примеру, встраивание рекомендаций, базирующихся на истории контактов с брендом, значительно увеличивает вероятность конверсии.

Следующим методическим направлением служит разработка качественного контента. Он должен быть не только информативным, но и вовлекающим. Результативные материалы (видео, статьи или интерактивные квизы) способны удерживать внимание аудитории, стимулировать ее к дальнейшим действиям.

Триггеры — это элементы, которые побуждают пользователя к тем или иным шагам. К ним относятся:

- временные ограничения;
- отзывы других людей;
- возможность получить уникальные предложения и т. п.

Важно учитывать, что их требуется органично «вписать» в структуру автоворонки и соответствовать ожиданиям аудитории.

В методологическом контексте очень значимо применение многошаговой сегментации аудитории, что предоставляет возможность создавать индивидуализированные пути взаимодействия. Задействование указанного подхода помогает принимать в учет потребности различных категорий пользователей. Например, новичкам уместно предлагать образовательные материалы, а постоянным клиентам — эксклюзивные решения.

Инструменты автоматизации (в частности, подразумеваются e-mail маркетинг, чат-боты, мессенджеры) обеспечивают поддержку постоянного контакта с клиентами на каждом этапе автоворонки [1]. При этом важно, чтобы сообщения оставались персонализированными, релевантными, в противном случае они зачастую утрачивают эффективность.

Наконец, среди методов целесообразно выделить постоянные проверки в виде тестов, а также анализ. Для улучшения исследуемых воронок необходимо проводить регулярное тестирование их элементов. К примеру, А/В-подход позволяет определить,

какой из вариантов заголовков, изображений, призывов к действию лучше работает с аудиторией.

С учетом отмеченного выше и ознакомления с современными научными публикациями предлагается авторское видение относительно оптимизации функционирования автоворонок в digital-маркетинге (рис. 3).



Рис. 3. Предложения по оптимизации автоворонок в цифровом маркетинге (составлено автором)

Fig. 3. Suggestions for optimizing autorocks in digital marketing (compiled by the author)

Комментируя представленную схему, следует подчеркнуть, что внедрение CRM позволяет объединять данные о клиентах из различных каналов, что облегчает построение индивидуальных маршрутов для каждого пользователя.



В свою очередь, чат-боты играют определяющую роль в автоматизации взаимодействия с потребителями, предлагая оперативные ответы на вопросы, направляя людей к нужным этапам автоворонки.

Элементы геймификации, опирающиеся на различные игровые механики (имеются в виду начисление баллов за активность, участие в викторинах), повышают вовлеченность аудитории, стимулируют ее к последующим действиям.

Наконец, предоставление бесплатных образовательных материалов (вебинаров, курсов, гайдов) не только укрепляет доверие клиентов, но и мотивирует их к участию в дальнейшем взаимодействии.

### **Выводы**

Резюмируя изложенное, целесообразно подчеркнуть, что в современном виде автоворонки представляют собой мощный инструмент автоматизации процессов в рамках digital-маркетинга, который помогает маркетологам привлекать, удерживать клиентов с минимальными затратами времени.

Успешное создание рассматриваемых в статье систем требует применения персонализированного подхода, задействования новых технологий в сфере аналитики, автоматизации, а также непрерывного тестирования всех этапов.

Описанные в работе методы и сформулированные рекомендации позволяют улучшить структуру автоворонок, повысить их результативность, адаптировать под потребности различных сегментов целевой аудитории.

В будущем исследование возможностей использования искусственного интеллекта, машинного обучения для управления характеризуемыми воронками представляется весьма перспективным направлением, дающим возможность достигать еще более высоких результатов.

### **Литература:**

1. Ботиенко А.В. Автоворонки продаж через чат-боты / А.В. Ботиенко, А.А. Федорина // Научно-технический прогресс. Задачи и их решения. Материалы международной научно-практической конференции. – Саратов: 2023. – С. 9-13.

2. Казарян С.А. Инновационные подходы к увеличению дохода через персонализацию и автоматизацию маркетинговых процессов: продуктовая матрица и автоворонки / С.А. Казарян // Молодой ученый. – 2024. – № 8 (507). – С. 56-58.



3. Купцова Д.М. Лучшие сервисы для построения автоворонок / Д.М. Купцова // Современные средства связи. – 2024. – Т. 1. – № 1. – С. 246-249.
4. Матасова О.И. Трансформация процесса продаж в образовательных учреждениях с помощью технологии автоворонок / О.И. Матасова, Д.В. Груне // Российская экономика в условиях структурной трансформации. Сборник материалов Всероссийской научно-практической конференции. – Москва: 2023. – С. 140-144.
5. Никуйко Е.А. Использование нейросетей в маркетинговой автоворонке продаж / Е.А. Никуйко, Н.Е. Прошкин // Радиотехника, электротехника и энергетика. Тезисы докладов Тридцатой международной научно-технической конференции. – Москва: 2024. – С. 666.
6. Пивкин Д. Автоворонка продаж – секреты эффективности и методики создания с нуля / Д. Пивкин // URL: <https://neiros.ru/blog/automation/avtovoronka-prodazh-sekretu-ehffektivnosti-metodiki-sozdaniya/> (дата обращения: 06.01.2025).
7. Татаринев К.А. Автоворонка на учебно-продающие интернет-консультации в массовом онлайн-обучении / К.А. Татаринев // Балтийский гуманитарный журнал. – 2020. – Т. 9. – № 2 (31). – С. 173-176.
8. Умаргалеева А.А. Использование метода «автоворонка продаж» при продвижении организации / А.А. Умаргалеева // Актуальные проблемы гуманитарных наук. Материалы Региональной научно-практической конференции. – Нижневартовск: 2020. – С. 264-266.
9. Цехомский А.В. Методология построения маркетинговых автоворонок в социальных сетях российского сегмента интернета / А.В. Цехомский, М.С. Вакуленко, Д.М. Касимова, И.В. Охотников // Московский экономический журнал. – 2022. – Т. 7. – № 10.
10. Шаманаев П.С. Роль автоворонок в сфере онлайн-образования / П.С. Шаманаев // Информационные технологии в современном мире – 2024. – Екатеринбург: 2024. – С. 63-66.



**Пиликина Е. А.**

Старший преподаватель

ФГБОУВО «Санкт-Петербургский государственный университет телекоммуникаций

им. проф. Бонч-Бруевича»

**Кулакова Ю. В.**

Студент 4 курс

Факультет «Радиоэлектронных систем и робототехники»

ФГБОУВО «Санкт-Петербургский государственный университет телекоммуникаций

им. проф. Бонч-Бруевича»

## **ИЗМЕНЕНИЕ КЛЮЧЕВОЙ ПРОЦЕНТНОЙ СТАВКИ, ЕЕ ВЛИЯНИЕ НА КРЕДИТЫ, ИПОТЕКУ И ВКЛАДЫ ЗА ВТОРУЮ ПОЛОВИНУ 2024 ГОДА**

Аннотация: Статья посвящена анализу изменений ключевой процентной ставки Банка России во второй половине 2024 года и их влиянию на инфляцию, кредитование, ипотеку и банковские вклады. Рассматриваются решения Центробанка по ужесточению денежно-кредитной политики, направленные на сдерживание инфляции и стабилизацию экономической ситуации.

В работе описаны причины повышения ставки, последствия отмены льготных программ, динамика роста процентных ставок по кредитам и вкладам.

*Ключевые слова:* ключевая процентная ставка, денежно-кредитная политика, инфляция, кредитование, ипотека, банковские вклады, Центробанк России, льготная ипотека, ужесточение условий, прогноз инфляции, процентные ставки.

*Keywords:* key interest rate, monetary policy, inflation, lending, mortgage, bank deposits, Bank of Russia, preferential mortgage, tightening measures, inflation forecast, interest rates.

### **1 Введение.**

Актуальность темы связана с влиянием ключевой ставки на инфляцию, экономическую стабильность и стоимость кредитов для бизнеса и граждан. В условиях глобальной нестабильности регулирование ставки обеспечивает устойчивость финансового рынка и банковской системы, отражая воздействие денежно-кредитной политики на экономику.



Центробанк принимает решения по ключевой ставке на специально проводимых заседаниях. В таблице 1 приведен список дат с запланированными заседаниями на 2024.

**Таблица 1. План заседаний Центробанка на 2024 год**

Дата заседания	Тип заседания
16 февраля	Опорное
22 марта	Промежуточное
26 апреля	Опорное
7 июня	Промежуточное
26 июля	Опорное
13 сентября	Промежуточное
25 октября	Опорное
20 декабря	Промежуточное

Изменение ключевой ставки во второй половине 2024 года рассматривается, поскольку этот период характеризуется усилением экономической неопределенности, влиянием внешних и внутренних факторов на инфляцию, а также активным использованием Центробанком инструментов денежно-кредитной политики для стабилизации финансового рынка.

## **2 Понятие процентной ставки.**

Процентная ставка — это плата за использование денежных средств, выраженная в процентах от суммы займа или депозита за определенный период времени. [1] Проще говоря, это процент, который заемщик выплачивает кредитору за возможность пользоваться его деньгами или который вкладчик получает за хранение средств в банке.

Ее изменение регулирует инфляцию и экономическую активность, определяя стоимость кредитов, ипотек и доходность вкладов. Повышение ставки удорожает кредиты, снижая спрос, а снижение — стимулирует заимствование. Для вкладчиков высокие ставки делают депозиты выгоднее, низкие — менее прибыльными. Таким образом, колебания ставки существенно влияют на финансовые решения и денежные потоки.

## **3 Предпосылки к отмене льгот по ипотеке, условия кредитов и вкладов июль – 1 августа 2024 год.**

В начале июля 2024 года процентная ставка составляла 16%.

1 июля 2024 года завершилась программа льготной ипотеки с господдержкой, по условиям которой взять ипотеку мог любой совершеннолетний гражданин РФ, соответствующий требованиям банка к доходу и кредитной истории. Ставка по льготе составляла 8 процентов годовых, при этом банки могли повысить ставку при отказе от



страхования жизни и здоровья не более чем на 1 процентный пункт. Ипотеку можно было оформить на покупку квартиры у застройщика по договору долевого участия (ДУУ) или по договору купли-продажи, частного дома, строительство частного дома, покупку земли для строительства частного дома. Максимальная сумма составляла 6 миллионам, а первоначальный взнос – не менее 30 процентов от стоимости жилья.

Отмена льготной ипотеки произошла из-за нескольких факторов, связанных с экономической ситуацией и влиянием программы на рынок недвижимости:

1. Рост ключевой ставки. Центральный Банк России повышает ключевую ставку для борьбы с инфляцией, что влияет на стоимость кредитов. Высокие ставки делали программу льготной ипотеки все более затратной для государства, так как субсидирование разницы между рыночной ставкой и льготной становилось все дороже.

2. Нагрузки на бюджет. Льготная ипотека требовала больших бюджетных средств на субсидирование ставок.

3. Высокий спрос на жилье. Льготная ипотека, запущенная для поддержки рынка жилья в условиях пандемии, привела к значительному росту спроса на жилье. Это вызвало стремительный рост цен на недвижимость, а программа увеличивала спрос, но предложение жилья росло медленнее.

4. Завершение программной цели. Первоначально льготная ипотека вводилась как временная мера для поддержки строительства и экономики в период пандемии. К 2024 году цели во многом достигнуты.

Ставки по вкладам также выросли до 18-19 процентов годовых в зависимости от условий и срока. Это можно охарактеризовать повышением ключевой ставки для борьбы с инфляцией: коммерческие банки вынуждены предлагать более высокие процентные ставки по вкладам, чтобы привлечь деньги от населения для бизнеса. В условиях повышенной инфляции и роста процентных ставок по другим финансовым инструментам банки сталкиваются с необходимостью конкурировать за капитал, что способствует удержанию и привлечению вкладчиков путем повышения ставки по депозитам.

В соответствии с планом 26 июля 2024 года прошло опорное заседание Центрального Банка, где Совет директоров Банка России принял решение повысить ключевую ставку на 200 б.п., установив ее на уровне 18,00% годовых. Это решение связано с ускорением инфляции, которая превысила апрельский прогноз. Существенный рост внутреннего спроса продолжает опережать возможности предложения товаров и услуг. Для снижения инфляции необходимо дополнительное ужесточение денежно-



кредитной политики, а для достижения целевого уровня — более строгие условия, чем ожидалось ранее. На ближайших заседаниях Банк России будет рассматривать возможность дальнейшего повышения ставки. Прогноз по инфляции на 2024 год пересмотрен в сторону повышения до 6,5–7,0%. При текущей денежно-кредитной политике в 2025 году годовая инфляция снизится до 4,0–4,5% и стабилизируется около 4% в долгосрочной перспективе. [2]

#### **4 Сохранение ключевой процентной ставки, сокращение IT-ипотеки, сокращение объема выдачи ипотеки, очередное повышение ставок по вкладам 1 августа – 1 сентября 2024 год.**

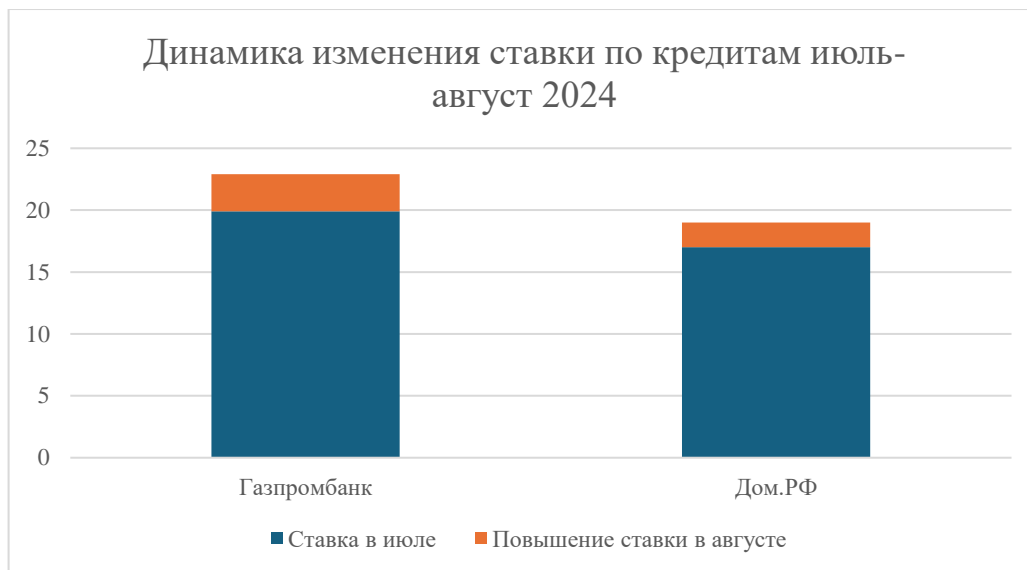
С 1 августа по 1 сентября 2024 года в России произошли важные изменения на финансовом рынке: сохранение ключевой процентной ставки, сокращение IT-ипотеки, снижение объемов выдачи ипотечных кредитов и очередное повышение ставок по вкладам. Эти меры являются частью политики Банка России по стабилизации экономики на фоне инфляционных рисков.

7 августа 2024 года Банк России принял решение о сохранении ключевой процентной ставки в 18 процентов. Однако денежно-кредитные условия ужесточились с июльского заседания, а средневзвешенные ставки продолжали расти и составили 20,6-21,6%. [3] Вследствие чего некоторые российские банки увеличили процентные ставки по потребительским кредитам. Например:

- Газпромбанк увеличил процентные ставки по потребительским кредитам на 3,5 п.п.: теперь годовая ставка начинается от 19,9%, а минимальная полная стоимость кредита (ПСК) достигает 23%.

- Банк «Дом.рф» поднял ставку на 2 п.п., установив их на уровне 19%.

На рисунке 1 наглядно показана динамика изменения процентных ставок вышеперечисленных банков.



**Рисунок 1. Изменение процентных ставок в августе в Газпромбанке и «Дом.Рф»**

*Источник: анализ автора*

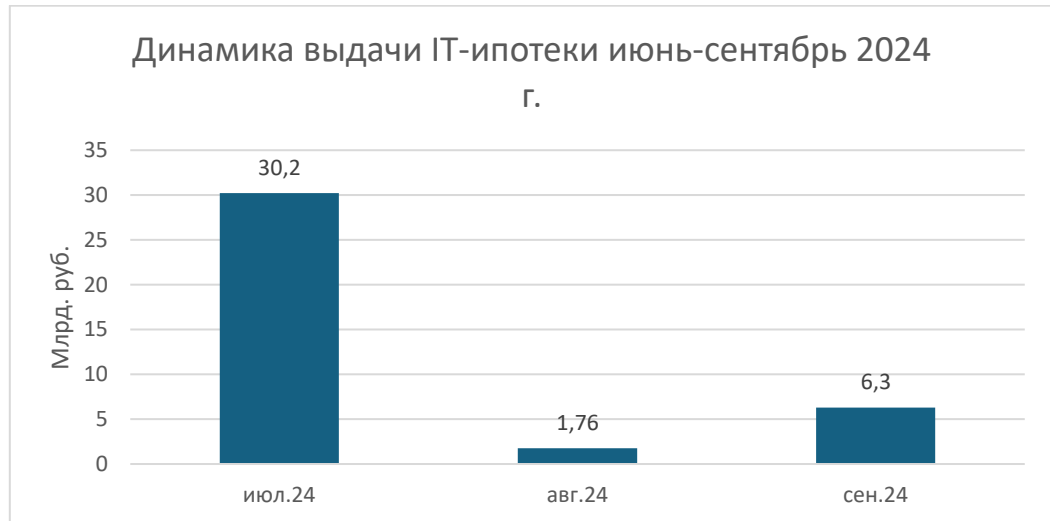
После отмены льготной ипотеки в июле снизился спрос на новостройки на 30%, а количество сделок упало на 52%.

Кроме того, в августе стало известно, что Центробанк может увеличить ключевую ставку до 20% годовых и выше. Предполагается, что снижение доступности ипотеки должно благоприятно повлиять на рынок недвижимости: улучшению качества строящегося жилья, так как застройщики не будут гнаться за покупателями и возводить квартиры с большим количеством маленьких квартир, по типу студий. На конец августа 2024 года взять ипотеку может человек с уровнем дохода не менее 300 тыс. рублей, что составляет всего 3% населения России.

Сокращение льготных программ, таких как IT-ипотека, существенно затрудняет покупку жилья для специалистов в сфере информационных технологий, которые ранее могли воспользоваться сниженной процентной ставкой. Ужесточение условий ипотечного кредитования также вызвано общим сокращением объемов выдачи ипотек в ответ на высокие риски невозврата долгов.

В августе 2024 года произошло сокращение выдачи IT-ипотеки в 17 раз: с 30,2 млрд. рублей до 1,76 млрд. рублей (по данным «ДОМ.РФ»). Это обусловлено тем, что с 1 августа Москва и Санкт-Петербург были исключены из госпрограммы, минимальная ставка увеличилась с 5% до 6%, а предельная сумма кредита для всех регионов была установлена на уровне 9 млн рублей. Теперь воспользоваться ипотекой можно только в регионах, максимальная сумма кредита уменьшилась в два раза. В Министерстве

цифрового развития России пояснили, что сокращение объёма выдач связано с перезапуском программы и увеличением её востребованности в регионах. На рисунке 2 можно наглядно увидеть спад выдачи ИТ-ипотеки с июля по сентябрь 2024 года.



**Рисунок 2. Спад выдачи ИТ-ипотеки июль-сентябрь 2024 года**

*Источник: анализ автора*

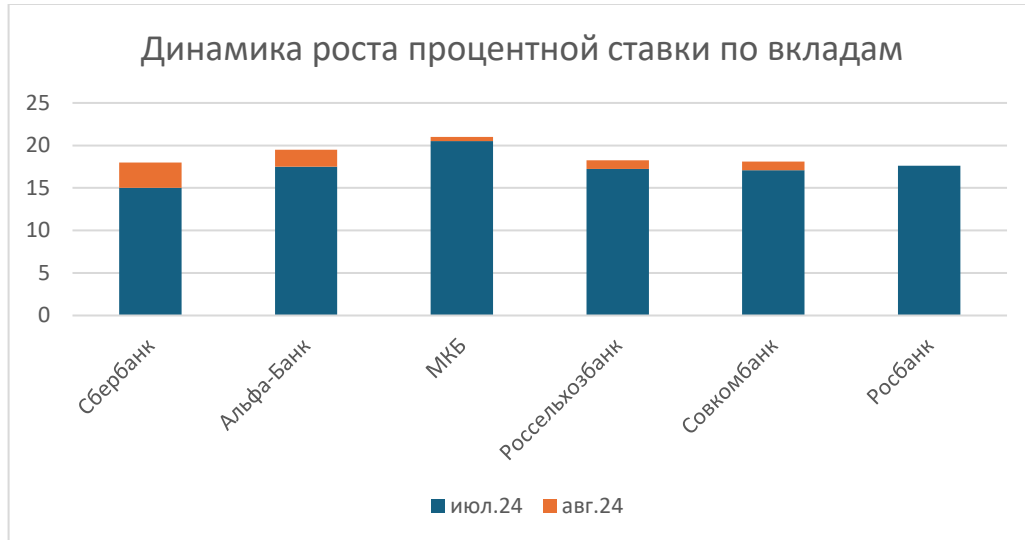
Одновременно банки повысили ставки по депозитам, чтобы привлечь средства от населения и бизнеса. В условиях роста процентных ставок вклады становятся более привлекательными, стимулируя граждан к сбережениям. В августе произошло повышение ставок по депозитам в среднем на 0,8-0,9 пунктов и возможная доходность в среднем достигла 18,5-19%. Ниже приведены изменения ставок по вкладам в крупных банках, а на рисунке 3 отображена данная динамика:

- Сбербанк увеличил ставки по вкладам на срок от трех до шести месяцев на 3 процентных пункта, предлагая максимальную доходность в 18%.
- Альфа-Банк поднял ставки по вкладам на аналогичный срок на 2 процентных пункта, доведя максимальный процент до 19,5%.
- Московский Кредитный Банк (МКБ) повысил ставки на три-шесть месяцев на 0,5 процентных пункта, с максимальной доходностью по полугодовому вкладу до 21%.
- Россельхозбанк увеличил ставки на 1 процентный пункт по депозитам сроком на три месяца, предложив максимальную доходность 18,25%.
- Совкомбанк поднял ставки по вкладам на три, шесть и двенадцать месяцев на 1 процентный пункт, с максимальной доходностью 18,1%, а по депозитам на три года ставка достигла 20% годовых.



- Росбанк повысил ставки по полугодовым вкладам на 0,4 процентных пункта, установив максимальную доходность на уровне 18%.

Более наглядно изменение ставок можно увидеть на следующем графике.



**Рисунок 3. Динамика роста процентной ставки по вкладам в вышеперечисленных банках**

*Источник: анализ автора*

Эти меры показывают стремление регулятора сдерживать инфляцию и снизить риски перегрева экономики, но они несут и определенные риски. Удорожание кредитов может привести к сокращению потребительской активности и инвестиционного спроса, что негативно скажется на росте экономики. Кроме того, снижение доступности жилья затруднит реализацию жилищных программ для населения и повысит социальную напряженность.

### **5 Промежуточное заседание Центробанка. Увеличение ключевой процентной ставки, прогнозы по ипотеке, кредитам в сентябре 2024.**

13 сентября 2024 года Банк России принял решение о повышении ключевой ставки 19% годовых. Объясняется это тем, что инфляция продолжает расти, а июльского увеличения ставки не хватило. Существенного роста ставок по депозитам ожидать не стоит. [4] Некоторые крупные банки, такие как Сбербанк и ВТБ, повысили проценты еще до заседания Центробанка. Остальные финансовые учреждения, вероятно, также корректируют условия по вкладам в сторону повышения. Подробнее о повышении ставок упоминалось в главе 4.

Также увеличатся ставки по кредитам и ипотеке, что сделает заемные продукты еще менее доступными.



Население и бизнес ожидают усиления инфляции, демонстрируя пессимистичные настроения в прогнозах. Это лишает регулятора возможности смягчить свою политику: когда существует ожидание ускоренного роста цен, усиливается спрос, что подстегивает инфляцию.

Высокие банковские ставки не приводят к значительному замедлению кредитования. Темпы роста розничного кредитования стали более сдержанными, что объясняется не только высокими ставками, но и сворачиванием льготной ипотеки и ужесточением условий предоставления займов.

Когда значительная часть заемщиков получает кредиты на льготных условиях с фиксированной ставкой, для остальных участников рынка ставки должны быть выше. Обратная ситуация также справедлива: по мере сворачивания льготных программ и ужесточения требований влияние ключевой ставки на рынок усиливается, что позволяет Банку России проводить более мягкую политику.

Сейчас регулятор считает, что замедление кредитования недостаточно, отмечая, что в корпоративном сегменте рост остается высоким. Это связано с тем, что значительную часть операций составляют менее чувствительные к рыночным ставкам — льготные кредиты, направленные на поддержку приоритетных для государства отраслей.

В результате власти уже обсуждают возможность скорого сворачивания таких льготных программ для бизнеса. Однако, пока этого не произошло, Банк России вынужден еще больше повышать ставку, что негативно сказывается на тех, кто не пользуется государственной поддержкой.

В преддверии решения по ключевой ставке инвесторы проявляли заметное беспокойство, поскольку регулятор не дал четких сигналов о своих планах. Прогнозы аналитиков и экспертов разделились: шансы на сохранение ставки на уровне 18% или повышение до 19–20% оценивались примерно одинаково. В условиях такой неопределенности фондовый рынок оставался под давлением.

В сентябре текущий уровень инфляции увеличился до 9,8% в годовом выражении, с учетом сезонных факторов, по сравнению с 7,5% в августе. Также базовая инфляция выросла до 9,1% после 7,7% в августе. Инфляционное давление, включая устойчивое, приближается к максимальным значениям с начала года. По состоянию на 21 октября годовая инфляция составила 8,4%, а к концу 2024 года ожидается в диапазоне 8,0–8,5%.

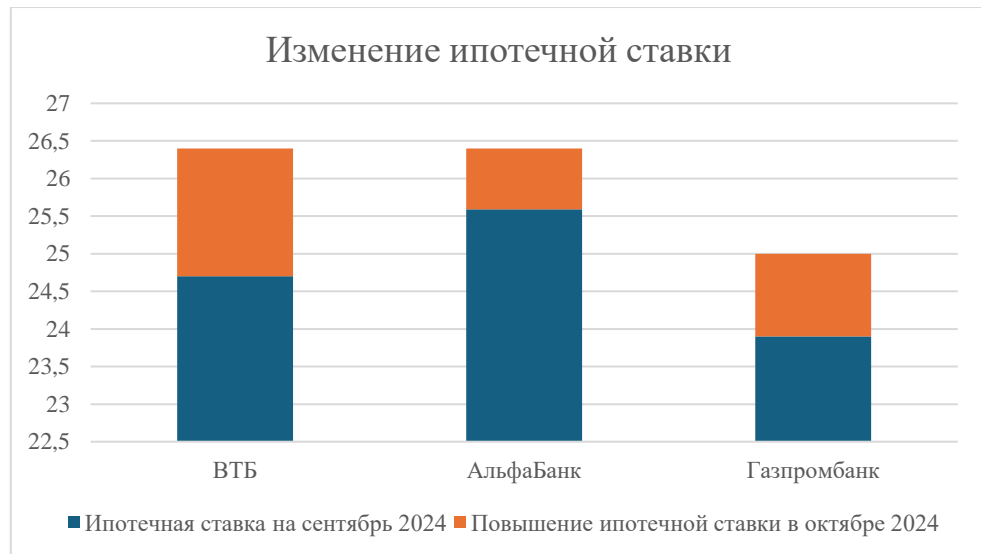


## **6 Опорное заседание Центробанка. Очередное повышение ключевой ставки октябрь 2024.**

25 октября 2024 года Совет директоров Банка России принял решение о повышении ключевой ставки на 200 б.п. до 21,00% годовых. Инфляция превышает июльский прогноз Банка России, инфляционные ожидания растут. Рост внутреннего спроса превышает предложение товаров и услуг, дополнительные бюджетные расходы увеличивают дефицит и имеют проинфляционные эффекты. «Требуется дальнейшее ужесточение денежно-кредитной политики, для того чтобы обеспечить возвращение инфляции к цели и снизить инфляционные ожидания.»[5]. Возможно повышение ключевой ставки на следующем заседании, которое анонсировали 20 декабря 2024 года. По прогнозу Банка России инфляция снизится до 4,5–5,0% в 2025 году и 4,0% в 2026 году, оставаясь на цели в дальнейшем. [5]

Инфляционные ожидания значительно возросли в октябре, достигнув максимумов с начала года. Население и бизнес реагируют на текущий всплеск инфляции. Краткосрочные и долгосрочные инфляционные ожидания аналитиков и финансового рынка также увеличились. Высокие инфляционные ожидания усиливают инерцию устойчивой инфляции.

Вместе с увеличением ключевой ставки в октябре 2024 года произошло замедление экономического роста и инфляции, что способствует усложнению для бизнеса привлечения и обслуживания кредитов, что может привести к замедлению развития и возможным банкротствам. Повышение стоимости обслуживания кредитов должно снизить потребительский спрос и удержать цены на товары и услуги на уровне. Доходность депозитов растет, так как процентные ставки в первой декаде месяца приблизились к 20% годовых. Ставки по кредитам растут, например, ипотечные ставки в Сбере выросли на 3 процентных пункта. Таким образом, минимальная ставка на вторичный рынок жилья выросла до 24,6%, а на первичный рынок – до 24,9 %. Также ипотечные ставки повысили банки ВТБ (24,7-26,4%), «АльфаБанк» (25,59-25,99%), «Газпромбанк» (23,9-25%). На рисунке 4 отображена динамика повышения ипотечной ставки для данных банков.



**Рисунок 4. Динамика роста ипотечной ставки в вышеперечисленных банках**

*Источник: анализ автора*

### **7 Промежуточное заседание Центробанка 20 декабря 2024 года.**

Совет директоров Банка России 20 декабря 2024 года решил сохранить ключевую ставку на уровне 21,00% годовых. Денежно-кредитные условия ужесточились в большей степени, чем предполагалось в октябре при предыдущем решении по ставке. Это стало следствием факторов, не связанных непосредственно с денежно-кредитной политикой. По оценке Банка России, с учетом существенного роста процентных ставок для заемщиков и снижения кредитной активности, текущие условия создают необходимые предпосылки для возобновления дезинфляционных процессов и возвращения инфляции к целевому уровню. Это возможно, несмотря на ускоренный рост цен и высокий внутренний спрос. На следующем заседании Банк России планирует оценить целесообразность дальнейшего повышения ставки, принимая во внимание динамику кредитования и инфляции. По прогнозу регулятора, в результате проводимой политики годовая инфляция снизится до 4,0% к 2026 году и в дальнейшем будет удерживаться на целевом уровне. [6]

Очередное заседание Совета директоров Банка России, посвященное обсуждению уровня ключевой ставки, намечено на 14 февраля 2025 года.

### **8 Заключение.**

Анализ изменений ключевой процентной ставки Банка России во второй половине 2024 года показывает, что денежно-кредитная политика регулятора стала значительно жестче в ответ на ускорение инфляции и рост внутреннего спроса. Принятые меры,



включая последовательное повышение ставки до 21,00% годовых, направлены на стабилизацию экономической ситуации и возвращение инфляции к целевому уровню.

Резкий рост процентных ставок повлиял на все сегменты финансового рынка. Ужесточение условий кредитования привело к сокращению объемов ипотечного кредитования, особенно в условиях отмены льготных программ. Одновременно увеличение ставок по вкладам стимулировало население к сбережениям, что помогло сократить потребительскую активность и снизить инфляционное давление.

В будущем ключевым фактором станет балансирование между необходимостью сдерживания инфляции и поддержкой экономической активности. Решения Банка России на предстоящих заседаниях будут зависеть от динамики инфляции, темпов кредитования и состояния финансового рынка.

#### **Литература:**

1. Процентная ставка. URL: <https://www.1mbank.ru/glossary/protsentnaya-stavka/>
2. «Банк России принял решение повысить ключевую ставку на 200 б. п., до 18,00% годовых» / Банк России. URL: [https://cbr.ru/press/pr/?file=26072024\\_133000Key.htm](https://cbr.ru/press/pr/?file=26072024_133000Key.htm)
3. «Резюме обсуждения ключевой ставки» / Банк России. URL: [https://cbr.ru/dkp/mp\\_dec/decision\\_key\\_rate/summary\\_key\\_rate\\_07082024/](https://cbr.ru/dkp/mp_dec/decision_key_rate/summary_key_rate_07082024/)
4. «Банк России принял решение повысить ключевую ставку на 100 б.п., до 19,00% годовых» / Банк России. URL: [https://cbr.ru/press/pr/?file=13092024\\_133000Key.htm](https://cbr.ru/press/pr/?file=13092024_133000Key.htm)
5. «Банк России принял решение повысить ключевую ставку на 200 б.п., до 21,00% годовых» / Банк России. URL: [https://cbr.ru/press/pr/?file=25102024\\_133000Key.htm](https://cbr.ru/press/pr/?file=25102024_133000Key.htm)
6. «Банк России принял решение сохранить ключевую ставку на уровне 21,00% годовых» / Банк России. URL: [https://cbr.ru/press/pr/?file=20122024\\_133000key.htm](https://cbr.ru/press/pr/?file=20122024_133000key.htm)



## Исторические науки



Чжэн Гуанцзе

Кандидат филологических наук, доцент  
Цзянсуский педагогический университет

Дай жуй

Студент  
Цзянсуский педагогический университет

**ДЕТСКАЯ ЛИТЕРАТУРА ПЕРИОДА ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ:  
ГЕРОИЗМ И ТРОГАТЕЛЬНАЯ БЕЗЗАЩИТНОСТЬ ЮНЫХ ЗАЩИТНИКОВ  
РОДИНЫ<sup>1</sup>**

Аннотация: В статье исследуется трансформация советской детской литературы в годы Великой Отечественной войны. Основной акцент сделан на смене тематики: героизм детей и взрослых, единство народа, трагедия преждевременного взросления. Анализируются произведения А. Гайдара, В. Катаева и других авторов, где сочетаются патриотический пафос и антивоенная риторика. Подчеркивается двойственная роль литературы: мобилизация через образы юных героев («сыны полка», партизаны) и гуманистическое осуждение войны, разрушающей детство. Рассматриваются психологические портреты детей, сохраняющих человечность в экстремальных условиях, а также ответственность взрослых за их судьбы. Примеры из фронтовой публицистики (очерки Гайдара, Маршака) иллюстрируют противоречие между необходимостью участия детей в борьбе и противоестественностью войны для детского мира.

*Ключевые слова:* Великая Отечественная война; героизм; детские писатели; детская литература.

*Key words:* the great patriotic war; heroism; children's writers; children's literature.

---

<sup>1</sup> В данной статье представлены промежуточные результаты общего проекта по подготовке студентов к предпринимательству и инновациям в провинции Цзянсу «Исследование политики социального обеспечения детей в России». 本文为江苏省大学生创新创业训练一般项目（自筹）“俄罗斯儿童福利政策研究”的阶段性成果。



Основной текст Великая Отечественная война полностью изменила жизнь советского государства и коренным образом поменяла тематику, идеологическую и эмоциональную составляющие детской книги.

В период Великой Отечественной войны перед детской литературой самой жизнью были поставлены новые задачи, в связи с чем изменилась тематика произведений. Основными стали:

- тема героизма детей и взрослых на фронте и в тылу;
- тема мужества народа и его сплочённости в борьбе с фашизмом;
- тема отношений войны и ребёнка.

Основная проблема, которой касались авторы, состояла в том, что война лишает ребёнка детства, меняет его судьбу. Дети взрослеют раньше, чем обычно, что не может не отражаться на их психологии, и в то же время они, благодаря высокой адаптивности, способны преодолевать все кризисы и вновь становиться обычными детьми.

Основной задачей детской литературы периода Великой Отечественной войны стало укрепление патриотического духа народа, изображение героических подвигов детей и взрослых как примера для подражания. В то же время война не показывалась как что-то нормальное. В детской литературе подчёркивалось, что она несёт много горя, меняет характеры, уничтожает семьи. Детская книга, как и вся советская литература этого периода (да и последующих) сочетала героический и антивоенный пафос.

Произведения этих лет были проникнуты верой в победу над врагом, любовью к народу и к Родине, которая в этот период понималась как СССР. Среди авторов, писавших для детей во время войны, можно назвать А.П. Гайдара, С.Я. Маршака, К.И. Чуковского, А.Т. Твардовского, З.Н. Александрову, М. Джалиля, А.Л. Барто, К.М. Симонова. Выдающимися являются произведения В.П. Катаева «Сын полка», Л.А. Кассиля «Улица младшего сына», Л.Ф. Воронковой «Девочка из города» и др. Во главу угла повествования стало такое понятие, как «судьбы детей» [1], причём судьбы по-взрослому непростые и всё же детские.

Многие детские писатели сражались в рядах действующей армии, активно работали во фронтовой печати. Они писали о несовместимости войны и детства, а одной из главных тем стала тема ответственности взрослых за судьбу детей в условиях войны. Можно назвать следующие статьи и очерки, вышедшие во время войны в периодической печати: А.П. Гайдара – «Война и дети», «Мост», «Переправа», С.Я. Маршака – «Родные дети», К.И. Чуковского – «Война и дети» и др.



К примеру, очерк А.П. Гайдара «Война и дети» был опубликован в газете «Комсомольская правда» 21 августа 1941 года. В нём описана встреча военных, отправляющихся на фронт, с несколькими детьми. Во-первых, – с пареньком, который угощает военных на станции смородиной, и его семилетним братишкой, образ которого показывает, как страшно соприкосновение детства и войны. На вопрос офицеров о том, что делают на войне, семилетний мальчик деловито отвечает: «Стреляют, <...> берут ружье или пушку, наводят... и бах! И готово» [2]. Мальчик спокойно описывает то, как война выглядит для него лично: «Пришел якийсь-то злыдень, бомбы на хаты швыряет, на сараи. Вот там бабку убили, двух коров разорвало» [Там же]. Он и его брат прекрасно разбираются в оружии, различают по звуку марки военных самолётов, и это одновременно восхищает и возмущает. Читатель не может не почувствовать, что дети, владеющие этой недетской информацией, выглядят неестественно и тревожно.

Ещё один герой очерка – подросток, занимающийся выпрашиванием у проезжающих мимо военных из отступающих и идущих на фронт частей патронов, чтобы помогать старшим – партизанам – сражаться с врагом. Герой очерка, офицер, верит мальчику и отдаёт ему свои патроны:

«Я смотрю ему в глаза. Я кладу ему в горячую руку обойму. Это – обойма от моей винтовки. Она записана на мне.

Я беру на себя ответ за то, что каждая выпущенная из этих пяти патронов пуля полетит точно в ту, куда надо, сторону» [Там же].

В очерке звучат противоречивые мысли: о несовместимости детей и войны, о недопустимости и ужасе такого совмещения и об уверенности в том, что дети могут принести пользу своей стране во время войны, могут воевать и уничтожать врага, пришедшего на их землю.

В прозе военных лет основными жанрами стали психологический рассказ и повесть. Основная проблема – исследование человека в критической ситуации в момент высокого напряжения духовной жизни.

Валентин Петрович Катаев (1897-1986) на протяжении своей жизни не раз обращался к творчеству для детей, но наиболее выдающимся его произведением, несомненно, является повесть «Сын полка», написанная в 1945 году. Основу сюжета произведения составляет судьба Вани Солнцева, потерявшего во время войны родителей и пережившего столько горя, сколько достаётся в жизни не всякому взрослому. Описание Вани таким, каким его впервые спящим в окопе увидели возвращающиеся из разведки



солдаты, трогательно и пронзительно: «Его непокрытая голова, заросшая давно не стриженными, грязными волосами, была неловко откинута назад. Худенькое горло вздрагивало. Из провалившегося рта с обметанными лихорадкой, воспаленными губами вылетали сиплые вздохи...» [Катаев 2015: 10]. Читатели видят Ваню глазами солдат и понимают, что им очень жалко мальчика, который столько пережил и которому совершенно не место на войне.

Перед читателем в образе Вани встаёт собирательный портрет обездоленного войной ребёнка: «Отец погиб на фронте в первые дни войны. Деревню заняли немцы. Мать не хотела отдавать корову. Мать убили. Бабка и маленькая сестренка померли с голоду. Остался один. Потом деревню спалили» [Там же: 29]. Однако беды не сломили мальчика, а только закалили его. Оказавшись среди бойцов капитана Енакиева, которые, поддавшись на уговоры Вани, делают его «сыном полка», он решил бороться с врагом как настоящий солдат. Солдаты искренне привязываются к мальчику, а сам капитан Енакиев считает его «названным сыном» [Там же: 243]. Только после гибели капитана Енакиева Ваня соглашается уйти с фронта в тыл – отправляется в суворовское училище.

В.П. Катаев рисует Ваню искренне желающим воевать, чтобы мстить отнявшему у него всё врагу. В то же время он показывает его обычным мальчиком, сохранившим в себе немало детских черт, которых он теперь стесняется. Например: «Чуть заметная улыбка, молодая, озорная, хитрая, скользнула по его губам» [Там же: 233].

Образ Вани Солнцева дан автором в переключке с образами героев старшего поколения, которые способны не только на безжалостные военные действия, но и на крепкую человеческую любовь. Повесть во многом психологична: писатель исследует внутренний мир ребёнка в условиях войны, жизнь и подвиг ребёнка на войне.

Если в книге «Сын полка» проблемы детского героизма и несовместимости ребёнка и войны сочетаются, то в книге Любви Фёдоровны Воронковой (1906-1976) «Девочка из города» на первый план выходит вторая из них. Здесь нет прямого изображения детского подвига и вообще действие происходит в тылу, но тема влияния войны на судьбу ребёнка звучит особенно остро.

Повесть была написана в 1943 году. Сюжетом стали события, обычные для лютых военных лет: оставшаяся сиротой беженка Валя (Валентинка) попадает в сельскую семью, где есть трое своих детей, отец воюет, а мать и дед много трудятся дома и в колхозе. Другие беженки рассказывают о девочке: «...Вся семья погибла. Отец – на фронте. А мать и братишка – здесь. Убиты...» [4, с. 5]. Позже оказывается, что мать с маленьким



братишкой на руках погибли прямо на глазах девочки. Валентинке предстоит не только привыкнуть к сельской жизни и стать своей в этой семье, превратиться в «дочку», но и забыть те ужасы войны, которые ей пришлось пережить. Вернее, не забыть их (это невозможно), а принять, понять, что жизнь продолжается и ещё может быть счастливой.

В повести удивителен образ матери, Дарьи, которая очень занята непростым сельским трудом, но находит время на внимание к каждому ребёнку. Именно её доброта и сердечность вернули Валентинке дом, радости детства, семью.

Ярко показаны отличия города и деревни, мешающие детям сразу принять Валентинку. Однако Л.Ф. Воронкова демонстрирует, что эти отличия не являются непреодолимыми, ведь детям в конце концов удаётся найти общий язык, подружиться и стать родными. Кстати, Валентинка лучше деревенской девочки Таиски управляет с домашними животными, искренне их полюбив. Это замечает дед: «Вот видишь, городская, а и то жалеет» [Там же: 34], который до этого сомневался: «Взять девочку? Ладно ли будет? <...> Мы деревенские, а она из города...» [Там же: 6].

Трогательно выглядит переписка Дарьи с воюющим на фронте мужем. Как бы невзначай, между другими известиями, мать сообщает мужу, что в доме теперь живёт Валентинка, и советуется с ним, стоит ли навсегда её оставить в семье. И, конечно, отец отвечает согласием: «...Ты, Даша, у меня умница и хороший человек. Не слушай, что говорят некоторые люди. Пускай сиротка найдет в нашем доме свой родной дом, пускай она в нашей семье найдет свою родную семью» [Там же: 68].

Девочка долго не может назвать Дарью мамой, расстраивая её этим. Девочка прекрасно помнит свою мать, и это кажется ей несправедливым. Но в итоге любовь побеждает, и книга заканчивается словами девочки, принесшей Дарье цветы: «Это я тебе принесла... мама!» [Там же: 72].

Итак, следует отметить, что советская детская литература в годы войны сыграла важную роль в патриотическом воспитании и отражении психологических аспектов детства в трудных условиях. Она стала средством мобилизации духа народа и проявления гуманизма в противостоянии с жестокостью войны. В период Великой Отечественной войны русская детская литература вынужденно переключилась на новые темы и проблемы, главной из которых стала проблема несовместимости ребёнка и войны. Тяжкие испытания, пришедшиеся на долю советского народа, не могли не отразиться на детской книге, её содержании и психологических особенностях.



**Литература:**

1. Борисова, М.С. Пейзаж в лирике В.А. Жуковского (на материале произведений, вошедших в круг детского чтения) / М.С. Борисова // Приволжский научный вестник. – 2015. – № 3-2 (43). – С. 34-37.
2. Гайдар, А.П. Война и дети / А.П. Гайдар [Электронный ресурс]. – URL: <https://www.litmir.me/br/?b=54375&p=1> (дата обращения: 17.02.2025).
3. Катаев, В.П. Сын полка / В.П. Катаев. – М.: АСТ, 2015. – 256 с.
4. Воронкова, Л.Ф. Девочка из города / Л.Ф. Воронкова. – М.: Детгиз, 1943. – 73 с.



## Педагогические науки



**Скляренко Ирина Вячеславовна**

Воспитатель

**Степанова Наталия Владимировна**

Воспитатель

**Филиппова Наталия Владимировна**

Воспитатель

МБДОУ «Детский сад №116 «Родничок»

города Чебоксары Чувашской Республики

**МЕТОДИЧЕСКАЯ РАЗРАБОТКА ПО ДОПОЛНИТЕЛЬНОМУ ОБРАЗОВАНИЮ В  
ДОУ КАК СТУПЕНЬ ДЛЯ РАЗВИТИЯ ДЕТЕЙ СТАРШЕЙ ГРУППЫ  
ПО ХУДОЖЕСТВЕННО-ЭСТЕТИЧЕСКОМУ РАЗВИТИЮ  
НА ТЕМУ: «КРАСКИ ОСЕНИ»**

Аннотация: В статье представлена Методическая разработка по дополнительному образованию в ДОУ как ступень для развития детей старшей группы по художественно-эстетическому развитию на тему: «Краски осени».

*Ключевые слова: художественно-эстетическое развитие.*

*Key words: artistic and aesthetic development.*

Большое значение для развития дошкольника имеет организация системы дополнительного образования в ДОУ, которое способно обеспечить переход от интересов детей к развитию их способностей. Развитие творческой активности каждого ребенка представляет главной задачей современного дополнительного образования в ДОУ и качества образования в целом.

**Цель:** Развитие творческих способностей детей через художественную деятельность.

**Задачи:**

– Совершенствовать технику вырезания симметричных предметов из бумаги, сложенной вдвое.



– Развивать чувство формы и композиционные умения (готовить элементы натюрморта в соответствии с величиной корзинки, размещать силуэты в корзинке, частично накладывая их друг на друга и размещая выше - ниже).

– Вызвать интерес к рассматриванию и самостоятельному созданию натюрмортов - многокрасочных, красивых, ярких. Подвести к пониманию того, что красивый натюрморт хорошо получается при сочетании разных цветов, форм и художественных техник.

**Предварительная работа:**

Воспитатель предлагает понаблюдать, как она сама вырезает силуэты из бумаги, сложенной вдвое (использует выразительную по цвету бумагу из старых журналов, буклетов). Изготовление корзинок теми детьми, которые не присутствовали на занятии по аппликации.

Рассматривание репродукций и художественных открыток с изображением натюрмортов, знакомство с натюрмортом как жанром живописи; рассматривание репродукций картин; составление натюрмортов из цветов, овощей, фруктов; рисование с натуры сухими художественными материалами (цветными карандашами, фломастерами).

**Материалы, инструменты, оборудование:**

Плетёные корзинки, подготовленные детьми на предыдущем занятии; квадратики и прямоугольники, вырезанные воспитателем из цветной бумаги (красного, жёлтого, оранжевого, синего, зелёного, персикового, фиолетового цвета), картон для фона; фактурная бумага для поиска новых цветосочетаний и оттенков, ножницы, коробочки для обрезков, клей, клеевые кисточки, салфетки, клеёнки; цветные карандаши и фломастеры для дополнения композиции.

**Наглядный материал:**

Репродукции натюрмортов: П.П. Кончаловского «Сирень в корзине», «Яблоки на столе у печки», И.И. Машкова «Снедь московская: хлебы», «Натюрморт. Синие сливы», И.Т. Хруцкого «Натюрморт» (фрагмент), «Цветы и плоды».

**Воспитатель:** Ребята, мы сегодня с вами попали в картинную галерею. Посмотрите внимательно, чем объединены все эти картины, в каком жанре они выполнены? (*Ответы детей*)

– Так, что же такое натюрморт?

**Воспитатель:** Натюрморт - это картина не только об особой жизни предметов, но и о людях, которые их изготовили, вырастили, собрали, об их отношении к этим вещам и о



том какие эти люди сами - добрые, трудолюбивые, заботливые, грустные или радостные, веселые или печальные.

Эта картина называется «Яблоки на столе у печки» художника П.П. Кончаловского. Посмотрите, как много яблок. Они спелые, сочные, только, что сорванные, нам кажется, что мы даже ощущаем их сладкий, медовый, тонкий аромат.

А это «Натюрморт» художника И.Т. Хруцкого. Посмотрите, как много грибов в этой корзиночке, несколько даже упало, на ножках грибов еще видны остатки земли. Главное в картине – корзина с грибами, художник поместил ее в центр. Чтобы сделать натюрморт еще наряднее художник положил около корзиночки несколько зеленых огурчиков.

Посмотрите на картину И.И.Машкова «Снедь московская: хлебы», она посвящена не только хлебу, но и человеку хлебобобу, землепашцу, пекарю. Потому что хлеб – это прежде всего труд, который в него вложили люди и в городе, и на селе.

А это «Натюрморт. Синие сливы.» художника И.И. Машкова. Тарелка с яркими синими сливами стоит в самом центре картины, на столе, она здесь самая главная. Сливы лежат по кругу тарелки, как бусы. А в центре слив, сверху лежит ярко-оранжево – красный крупный персик. Вокруг тарелки тоже красуются красные, оранжевые, желтые персики. Картина очень нарядная. Цвет фона и стола серовато – белый, он не мешает видеть фрукты, а наоборот подчеркивает их красоту.

Обратите свое внимание на картину П.П. Кончаловского «Сирень в корзине». Посмотрите, какая красивая сирень. Как она хорошо смотрится собранная в один большой букет. Сирень только что собрали, чтобы поставить в вазу. Она свежая и душистая.

*Воспитатель подводит детей к столу, на котором стоит корзина с фруктами накрытая тканью.*

**Воспитатель:** Ребята, посмотрите, что здесь спрятано, (*убирает ткань*) что это?  
(*Ответы детей*)

Дети рассматривают красивый натюрморт из качественных муляжей, который помещён на столе. Воспитатель предлагает детям не спеша обойти натюрморт и рассмотреть его со всех сторон. Обсуждаются наблюдения и выводы детей о том, что натюрморт с разных сторон выглядит по-разному (если посмотреть с одной стороны, на переднем плане груша, а если посмотреть с другой стороны, на переднем плане яблоко и т.д.). Воспитатель показывает детям два-три натюрморта в плетёных корзинках. Предлагает полюбоваться и напоминает, что дети уже подготовили корзинки для таких красивых натюрмортов.



**Воспитатель:** Сегодня на занятии мы будем вырезать разные фрукты и составлять из них красивые натюрморты в наших плетёных корзинках. Давайте поговорим о том, какие фрукты и как мы сможем вырезать.

Воспитатель показывает детям бумажный прямоугольник и квадрат и предлагает подумать, из какой формы лучше всего вырезать грушу, а из какой - яблоко. После ответов детей напоминает способы вырезания (аппликация симметричная, ленточная, по нарисованному контуру, обрывная).

Дети находят свои плетёные корзинки, выполненные на предыдущем занятии. Они обдумывают свои замыслы и начинают работать. Воспитатель помогает косвенными вопросами, эмоционально поддерживает, при необходимости подводит ребенка к способу поиска или выбору цветовой гаммы.

Дети вырезают силуэты фруктов и помещают их в свои плетёные корзинки. Если фрукты не помещаются в корзинке, воспитатель советует частично наложить силуэты друг на друга и подвигать в поисках лучшего их размещения. Воспитатель подсказывает, что готовую композицию можно дополнить красивыми листочками, колосками, бабочками, стрекозами, жуками вырезать и наклеить или нарисовать цветными карандашами, фломастерами, красками.

Дети любят свои натюрморты.



Алексеева Людмила Ивановна

Учитель английского языка

МБОУ Момская СОШ

## СТРАТЕГИЯ ПОДГОТОВКИ К ВЫПУСКНЫМ ЭКЗАМЕНАМ ОГЭ И ЕГЭ ПО АНГЛИЙСКОМУ ЯЗЫКУ

Аннотация: Единый государственный экзамен по английскому языку - это важный и ответственный выбор. Подготовка к успешной сдаче ОГЭ И ЕГЭ является серьезным и долгосрочным проектом. Обучающимся необходимо:

- системно заниматься английским языком
- много слушать и читать
- разбираться в лексических и грамматических явлениях языка.

*Ключевые слова:* ЕГЭ по английскому языку, системный подход, система оценивания заданий, план, пробные экзамены и тесты, планирование времени, мотивация.

*Keywords:* USE in English, a systematic approach, a task assessment system, a plan, mock exams and tests, time planning, motivation.

Подготовка к ОГЭ и ЕГЭ по английскому языку требует системного подхода. В своей статье хочу раскрыть некоторые стратегии, которые помогут успешно сдать экзамен.

**1. Понимание формата экзамена.** Надо ознакомиться с форматом и структурой заданий ОГЭ и ЕГЭ.

**2. Понимание системы оценивания заданий.** Познакомьтесь с критериями, дополнительными схемами развернутых ответов при выполнении типовых заданий.

**3. План.** Разработайте план подготовки к экзамену. Для этого нужно определить слабые и сильные стороны своих знаний и разработать план подготовки, уделяя побольше внимания на свои слабые места.

**4. Лексика и грамматика.** Расширяйте активный словарный запас. Систематизируйте грамматические правила языка.

**5. Чтение.** Читайте тексты разной сложности. Умейте выделять основную информацию и детали, факты.



6. **Письмо.** Практикуйтесь в написании различных типов письменных работ (сочинение, письма). Обратите внимание на структуру и логику изложения.

7. **Аудирование.** Слушайте различные аудиоматериалы включая разговоры, лекции, интервью. Учите словарный минимум и выражения, используемые в разговорной речи.

8. **Устная часть.** Тренируйте навыки ответов на вопросы по темам экзамена. По возможности, записывайте себя, анализируйте произношение и грамматику.

9. **Пробные экзамены и тесты.** Регулярно сдавайте и анализируйте свои ошибки. Следите за временем, при сдаче тестов старайтесь соблюдать временные рамки. Особенно при устной части экзамена и при написании эссе.

10. **Планирование времени.** Распределяйте время на подготовку по разделам экзамена. Помните по разделам, в основном, по 30 минут. Создайте самостоятельно график подготовки.

11. **Мотивация.** Ставьте цели и поощряйте себя при выполнении.

Поддерживайте положительный настрой и верьте в свои силы.

Подготовка требует регулярной практики и требует систематического подхода. Усердие и целенаправленная работа приведут к успеху.

**Разберем эти аспекты более подробно.**

### **1. Понимание формата экзамена:**

- Анализ структур и особенностей каждого раздела экзамена (аудирование, чтение, письмо, устная часть).

- Ознакомление с правилами оценивания и требованиями к каждому типу задания.

- Выделение основных тем, которые могут встретиться в различных разделах

### **2. Разработка плана**

- Подробное описание текущих знаний языка.

- Оценивание количества доступного времени до экзамена и распределение на подготовку к каждому разделу.

- Указание конкретных методов изучения (чтение книг, прослушивание аудиозаписей, учебники по грамматике)

### **3. Лексика и грамматика**

- Создание тематических словарей по темам, которые встречаются в экзаменах (образование, технологии, здоровье, охрана окружающей среды и т.д.)



- Регулярно обновлять и расширять свой словарный запас новыми словами и фразами.

- Составление графика изучения грамматических правил ( выделить основные темы )

#### **4. Чтение**

- Отработка навыков быстрого чтения

- Практика навыков определения основной идеи текста, выделение ключевых аспектов текста.

- Регулярное решение тестов и заданий , проверяя свои результаты.

#### **5. Письмо**

- Отработка структуры эссе: введение, основная часть , заключение.

- Тренировка в написании эссе по предложенным темам, соблюдая ограничение по количеству слов и времени.

- Обратная связь с учителем , чтобы улучшить структуру и стиль письма.

#### **6. Аудирование**

- Слушание разнообразных аудиоматериалов: аудиокниги, интервью, диалоги.

- Поддержка словарного запаса, отслеживая из прослушанных текстов.

- Практика в понимании основной информации и деталей.

#### **7. Устная часть**

- Тренировка ответов на типичные вопросы по аудированию.

- Запись ответов и повторное прослушивание , обращая внимание на правильность и разнообразие лексики

- Отработка ответов в выражении собственного мнения и аргументации.

#### **8. Проведение пробных экзаменов.**

- Проведение пробных тестов в условиях, максимально приближенных к настоящим экзаменам.

- Анализ ошибок и уточнение слабых сторон для дальнейшей подготовки

- Работа над стратегиями ответов в условиях ограниченного времени

#### **9. Планирование времени**

- Составление графика подготовки на небольшие блоки

- определение периодов отдыха и пересмотров пройденного материала

- Использование приложений и инструментов для управления временем

10. Обратная связь.



- Регулярное общение с учителем
- Обсуждение вопросов и устранение пробелов
- Применение обратной связи для коррекции стратегий и улучшения навыков.

### **11.Самомотивация**

- Запись своих достижений и прогресса
- Использование разнообразных источников мотивации (успехи, цитаты, образцы хороших работ )
- Создание системы поощрения для себя после достижения целей.

Экзамен проверяет не то, что вы знаете об языке, а как вы можете использовать иностранный язык: слушать и понимать, читать и понимать, использовать грамматические формы и лексику в соответствии с коммуникативным заданием, писать личное письмо и письменное высказывание с элементами рассуждения.

Выше перечисленные стратегии развивают все языковые навыки и речевые умения, необходимые для успешной сдачи выпускных экзаменов по английскому языку.

Обычно надо начинать интенсивную подготовку с 10 класса. Вот несколько **советов** как начать подготовку.

- Проведение входного тестирования. Лучше использовать демоверсию ФИПИ. Вы понимаете уровень ученика и его сильные и слабые стороны. Еще посмотрите, готов ли он работать серьезно.

- Если до экзамена мало времени, а уровень невысокий отдельный УМК не поможет. Лучший вариант будет разбор грамматики и лексики плюс шаблоны письма и говорения. Также отдельно отработать словообразование и подсказать стратегию для выполнения аудирования и чтения. Даю тесты на каждом занятии, то есть раз в неделю. Но перед экзаменами можно проводить занятия через день.

- Если до экзамена есть два года, а уровень невысокий, то весь десятый класс работаю над повышением уровня языка. Можно в 11 классе, также продолжить уровень языка.

- Перед экзаменом уделить время стратегиям, научить мыслить и размышлять. Это особенно полезно при написании задания 40.1 и 40.2 (написание письма и сочинения и в 4 задании устной части экзамена.

- Помнить ЕГЭ – это шаблоны и четкие инструкции. Никакой самодеятельности, следовать четко этим инструкциям.



- Обращать внимание на то, что лучше удается ученику. Можно сильно не переживать по 1 заданию в устной части – чтения текста (1 балл).
- Надо убедить ученика, что итоговый результат зависит не только от учителя, а от самого ученика. Как он посещает консультации, выполняет задания самостоятельно, желаемого количества баллов, мотивации также зависит результаты экзамена.

**Результаты экзаменов по английскому языку**

Год	Экзамен	Результат	Оценка
2015	ОГЭ	48	4
2017	ОГЭ	48	4
2017	ОГЭ	54	5
2017	ЕГЭ	64	3
2023	ЕГЭ	85	5
2023	ОГЭ	36	3

**Литература:**

1. М.В.Вербицкая, К.С. Махрумян, Е.Н. Нечаева  
Я сдам ЕГЭ! Английский язык. Практикум и диагностика. Москва  
« Просвещение » 2017 г.
2. Т.А. Кузнецова ЕГЭ: Грамматика и лексика. Подготовка и тесты. Издательство  
MMI Publications. 2017г.
3. Е.Р. Ватсон Всероссийская проверочная работа. Английский язык. М.:  
Издательство « Экзамен » , 2023



Ташлык Вика Александровна

Учитель начальных классов

КГУ «Мичуринская средняя школа»

## **ФОРМИРОВАНИЕ ИССЛЕДОВАТЕЛЬСКИХ УМЕНИЙ МЛАДШИХ ШКОЛЬНИКОВ ЧЕРЕЗ ПРОЕКТНУЮ ДЕЯТЕЛЬНОСТЬ НА УРОКАХ ЕСТЕСТВОЗНАНИЯ**

Аннотация: В данной статье рассматривается процесс формирования исследовательских умений младших школьников через проектную деятельность на уроках естествознания. Актуальность исследования обусловлена необходимостью разработки эффективных методов обучения, способствующих развитию критического мышления, инициативности и интереса к предмету. Приведены примеры проектной деятельности, определены её основные преимущества и указаны рекомендации для педагогов.

*Ключевые слова: естествознание, проектная деятельность.*

*Keywords: natural sciences, project activity.*

В современном обществе, где наука и технология играют все более важную роль, формирование у детей исследовательских умений является крайне актуальной задачей. Эти умения позволяют детям стать более знающими, уверенными, самостоятельными, творческими и готовыми к решению сложных проблем. Это связано с тем, что в условиях интенсивно развивающегося мира важно, чтобы уже в раннем возрасте дети начинали проявлять интерес к исследованию окружающего мира и развивали соответствующие навыки. Титанические достижения в педагогике связаны с именем педагога Я. А. Коменского. В его трудах вырисовывается некая двойственность: в первом случае он придерживался философии сенсуализма, а с другой стороны разработал нововведение, не позволяющее использовать исследовательский метод обучения в образовательной практике. Непосредственно сам «метод проектов» вступает в силу с 20-х годов прошлого столетия в Соединённых Штатах Америки. Основоположником является Д. Дьюи (американский педагог, философ, психолог), а его последователь У.Килпатрик. Они предложили вести обучение через теоретические концепции прагматической педагогики и провозгласили «принцип посредством делания». В данный период развития общества



требуются всесторонне развитые личности, умеющие адаптироваться в любых условиях жизни, быть мобильными. Учёные пришли к выводу, что этому может поспособствовать применение проектной деятельности на уроках для развития исследовательских умений.

Исследовательские умения можно определить, как способность самостоятельно организовывать исследовательскую деятельность, выявлять проблему, ставить цель и гипотезу, а также анализировать и обобщать результаты исследования. В младшем школьном возрасте эти умения начинают формироваться через практическую деятельность, включая проектную работу.

Проектная деятельность является мощным инструментом для формирования исследовательских умений. Она позволяет детям не только применять знания на практике, но и учит их работать в группе, искать информацию, формулировать вопросы и выводы. Важной особенностью проектной работы является то, что она направлена на активное исследование, а не на пассивное усвоение материала. Проектная деятельность на уроках естествознания способствует развитию у младших школьников навыков работы с природными явлениями и их исследования в условиях школьного эксперимента. Проектная деятельность как метод обучения включает в себя активное вовлечение обучающихся в процесс исследования, что позволяет им самостоятельно формулировать задачи, разрабатывать методы их решения и презентовать результаты. В основе проектной деятельности лежит конструктивизм, который акцентирует внимание на том, что знания лучше усваиваются, когда учащиеся находятся в активной познавательной позиции.

Проектная деятельность в контексте уроков естествознания включает различные формы работы, такие как создание научных проектов, проведение экспериментов, наблюдения за природными явлениями. Одним из важных аспектов проектной работы является то, что она дает учащимся свободу выбора темы исследования, что способствует развитию их творческого потенциала.

Проектная деятельность на уроках естествознания может включать как индивидуальные, так и коллективные формы работы. В обоих случаях учащиеся становятся участниками исследовательского процесса, начиная с постановки цели и заканчивая анализом результатов. Например, проект "Жизнь растений в разных условиях" позволяет детям исследовать, как различные условия окружающей среды влияют на рост растений. Этот опыт помогает школьникам развить навыки наблюдения, экспериментации, сбора данных и анализа информации.



Проектная деятельность также способствует формированию навыков критического мышления и самостоятельности. Как отмечает педагог М.И. Махмутова, "в процессе работы над проектом учащиеся сталкиваются с необходимостью самостоятельно искать ответы на вопросы, что способствует развитию их аналитических способностей" [1].

Исследовательские умения включают в себя:

- **Формулирование вопросов:** умение задавать поисковые вопросы, которые требуют анализа и исследования.
- **Сбор и анализ информации:** навыки работы с различными источниками данных.
- **Экспериментирование:** способность проводить простые эксперименты для проверки гипотез.
- **Оформление и представление результатов:** умение документировать и представлять результаты своего изучения в графическом и текстовом виде.

На уроках естествознания для формирования исследовательских умений младших школьников можно реализовать следующие проекты:

- **Проект "Экологический след":** Учащиеся исследуют влияние своей деятельности на окружающую среду, собирая данные о потреблении воды, электроэнергии и производстве отходов. Результаты оформляются в виде презентации и обсуждаются на уроке.
- **Проект "Мир насекомых":** Дети исследуют различные виды насекомых в своём районе, собирая информацию о их среде обитания и роли в экосистеме. Это может включать наблюдения, щелчки и видеосъёмки, а также создание буклетов или плакатов о насекомых.
- **Проект "Разнообразие растений":** В этом проекте учащиеся изучают различные виды растений, исследуют, как они растут и развиваются в различных условиях. Результаты могут быть представлены через изготовление альбомов или буклетов.

Для формирования исследовательских умений младших школьников через проектную деятельность на уроках естествознания я использую следующие приёмы:

- Предложение учащимся сформулировать вопросы по изучаемой теме и найти на них ответы с помощью экспериментов или исследований.



- Проведение домашних мини-исследований, где ученики должны собирать информацию по заданной теме (например, изучение экосистемы своего двора).
  - Создание групповых проектов, в рамках которых дети могут разрабатывать свои темы, планировать этапы работы и представлять свои результаты в виде презентаций, постеров или буклетов.
  - Использование накопительных проектов, где учащиеся накапливают данные и результаты исследований на протяжении учебного года.
  - Обучение работе с различными источниками информации (книги, статьи, интернет-ресурсы), чтобы дети научились находить и обрабатывать данные.
  - Создание библиотечки для самостоятельного чтения и исследования тем на уроках естествознания.
- деятельность**
- Проведение простых экспериментов, исследование явлений природы (например, изучение процессов фотосинтеза, исследование свойств воды), что позволяет детям делать выводы на основе наблюдений.
  - Использование опытов, связанных с повседневной жизнью (например, изучение роста растений в разных условиях).
  - Проведение ролевых игр, где ученики могут взять на себя различные роли (например, исследователи, учёные, экологи) и обсуждать важные вопросы, касающиеся изучаемых тем.
  - Использование интерактивных игр для изучения экологии, географии или биологии, которые фиксируют интерес учащихся.
  - Организация дискуссий по актуальным вопросам, связанным с природой и экологией, что требует от учеников анализа проблем и формулирования своих мнений.
  - Проведение дебатов на темы, связанные с охраной окружающей среды или использованием природных ресурсов.
  - Применение различных форматов для представления результатов работы (плакаты, мультимедийные презентации, графические схемы), что помогает развивать художественные и исследовательские навыки.
  - Создание журналов исследований или альбомов, где учащиеся могут документировать свои выводы и рисовать наблюдаемые явления.
  - Обучение детей планированию своих проектов: составление плана, определение целей, задач и сроков выполнения.



➤ Применение самооценки: дети могут оценивать свои достижения, обсуждать, что им удалось, а что можно было бы улучшить.

Таким образом, проектная деятельность является важным инструментом для формирования исследовательских умений у младших школьников на уроках естествознания. Она способствует развитию у детей навыков самостоятельной работы, анализа, критического мышления, а также формирует у них интерес к науке и исследовательской деятельности. Важно, чтобы проектная деятельность была интегрирована в учебный процесс и соответствовала возрастным особенностям учащихся. Это поможет не только повысить качество образования, но и создать условия для формирования исследовательской культуры у детей. Также это поможет ученикам стать более готовыми к жизни и к сложным проблемам, с которыми они столкнутся в будущем. Они смогут применять свои исследовательские навыки, чтобы решить эти проблемы и сделать свой вклад в развитие науки и технологии. Такой подход позволяет ребятам более глубоко познавать мир науки и развивать свои творческие способности, что в дальнейшем может стать основой для успешной научной карьеры.

#### **Литература:**

1. Махмутова, М.И. Формирование исследовательских умений у младших школьников через проектную деятельность. — М., 2018.
2. Дружков, В.Н. Психология проектной деятельности младших школьников. — СПб., 2016.



**Постивая Нелли Николаевна**

Преподаватель

Приднестровский государственный институт искусств

им. А. Г. Рубинштейна, г. Тирасполь

**Спивак Илона Анатольевна**

Преподаватель

Приднестровский государственный университет им. Т.Г. Шевченко

## **ИСТОРИЧЕСКИЕ АСПЕКТЫ АКТИВНОСТИ МОЛОДЕЖИ В РАМКАХ ХОРЕОГРАФИЧЕСКОГО КОЛЛЕКТИВА**

*Аннотация:* В данной статье рассматриваются аспекты педагогической и творческой работы руководителя самодеятельного хореографического коллектива, Заслуженного деятеля искусств МССР Бориса Решетникова. Акцентируется внимание на творческом развитии коллективов народного танца городов Бендеры и Тирасполь.

*Ключевые слова:* самодеятельный коллектив, хореография, творческая и педагогическая деятельность.

*Abstract:* This article examines aspects of the pedagogical and creative work of the head of the amateur choreographic group, Honored Artist of the Moldavian SSR Boris Reshetnikov. The focus is on the creative development of folk dance groups in the cities of Bendery and Tiraspol.

*Keywords:* amateur group, choreography, creative and pedagogical activity.

В настоящее время актуальным становится гиподинамия молодежи, которая основное время проводит в гаджетах. Уже в современных условиях стало запрещено использование на уроках телефонов, что отвлекает учащихся от образовательного процесса, дети и молодежь после занятий также не стремятся заниматься двигательной активностью, так как большое разнообразие спортивных и двигательных направлений представлено в цифровом формате, где не надо затрачивать много сил и времени. Для изучения данного вопроса, можно обратиться к историческим аспектам заинтересованности молодежи в СССР на территории современного Приднестровья.

В период развития коллективов художественной самодеятельности в стране были созданы все условия, на реализацию планов отпускались огромные средства, к работе с



самодеятельными артистами привлекались лучшие профессиональные силы страны – режиссеры, балетмейстеры, художники, артисты и педагоги. Совместные сценические выступления деятелей культуры и искусства МССР и УССР тогда не были редкостью. В Молдавской республике, как и по всей стране, активно велась работа по набору талантливой молодёжи в коллективы художественной самодеятельности. Появление квалифицированных специалистов, в числе которых был и Б.Решетников, все ждали с особым интересом.

Сфера деятельности начинающего руководителя включала организацию самодеятельных коллективов хореографической направленности в городах Бендеры и Тирасполь, выполнение наставнических функций, проведение репетиционных работ, подбор репертуара коллективам, формирование их стилистической и сценической узнаваемости. Кроме творческого руководства, предстояло решение практических вопросов таких, как выбор музыкальных произведений, костюмов, планирование гастрольной деятельности.

Артист Одесского театра оперы и балета, начиная свою работу в качестве руководителя хореографического коллектива, первоочередной задачей считал повышение уровня сценической, танцевальной и музыкальной культуры. Грамотный и логически выстроенный процесс работы, владение педагогическими навыками способствовали эффективности обучения и повышению профессионального уровня хореографических коллективов. Экзерсису у станка он всегда отводил решающую роль в подготовке высококлассных артистов народного танца. Формирование телосложения, физической и психической собранности, развитие силы, гибкости и эластичности мышц, улучшение координации движений, развитие чувства ритма и вестибулярного аппарата, а также устойчивости стали главным в решении поставленных руководителем задач.

В самодеятельном коллективе учебный процесс имеет свои специфические черты, его большая часть времени связана с концертной деятельностью, поэтому Борис Решетников, учитывая его особую специфику, опирался на те принципы обучения, которые способствовали физическому совершенствованию личности каждого участника коллектива, воспитывали хореографическое мышление, музыкальность, художественный вкус, чувство прекрасного, помогающего правильно оценивать явления жизни и искусства. Это педагогические принципы, выстраивающиеся на активности, наглядности, доступности, систематичности и прочности знаний.



Работая над технически сложными танцевальными элементами, он добивался не только точного, но и осознанного, выразительного исполнения. Наделённый необыкновенным внутренним миром, талантом и способностью творить, он осуществил ряд постановок, которые обогатили и разнообразили уже сложившийся к тому времени репертуар ансамблей народного танца. В книге Л. Ошурко «Народные танцы Молдавии», изданной в 1957 году, описаны самые интересные и распространённые в республике танцы. Постановка Бориса Решетникова «Чобэнаш» вошла в её содержание.

За достигнутые успехи и хорошую подготовку коллективов к окружным и республиканским смотрам художественной самодеятельности в 1952 году Борису Решетникову была вручена Почетная грамота Президиума Верховного Совета МССР. Такие постановки, как русская «Кадриль» и «Плясовая», молдавская «Хора фетелор», «Сус-опинка», «Молдовеняска», румынский «Плуташи» и многие другие, помогали коллективам обрести свое лицо и неповторимый стиль исполнения.

Профессиональная позиция руководителя, включающая ведущие методы и формы обучения и воспитания, позволяла участникам коллективов не только овладевать основами хореографии, но и углублять знания в этой области, делая их всесторонними, связывая танец с широким кругом явлений искусства и жизни. Желавших заниматься танцевальным творчеством становилось с каждым годом всё больше. Привлекал высокий профессионализм и ответственное отношение к работе его руководителя.

Наделенный творческой инициативой, педагогическими, организаторскими и аналитическими способностями, Борис Решетников предвидел дальнейшее построение педагогического и воспитательного процесса, востребованность репертуара, направление развития коллектива и создание творческой атмосферы в нем.

Обладая большой практикой работы с классическим репертуаром, он понимал, что для создания поистине уникальных по своей природе танцев необходимы знания молдавского фольклора, его особенностей и колорита. Для наполнения хореографических композиций образной поэтикой народного танца и органичного выражения в танцевально-пластической хореографии, необходимо было владеть спецификой этого вида танца, не забывая о его предназначении, и как основе хореографического искусства.

Изучая и осваивая методику исполнения танцев народов СССР и народов социалистических стран, Борис Решетников, прежде всего, повышал свой уровень образования. Прислушиваясь к мнению коллег, анализируя, он принимал, как показывало время, всегда верные решения. Постоянное желание создавать помогало рождению и



воплощению на сцене поистине ярких композиций, главным в которых являлось внутреннее содержание, сохранение народной основы, отражение развития рисунка, исполнительское мастерство участников коллектива, художественное оформление и правильное решение костюма.

Постепенно в коллективах складывались и традиции постановок танцев народов социалистических стран. Они вносили красочное многообразие в концертные программы и в тоже время помогали артистам осваивать различные стили, манеру исполнения, способствуя тем самым обогащению молдавского народно-сценического танца [1].

Организация работы, знания и опыт руководителя способствовали становлению и развитию коллективов, о которых стали говорить не только на родине, но и далеко за её пределами. Такой подход к проведению занятий развивал способности участников и давал возможность исполнять композиции, различные по видам и жанрам.

В репертуаре коллективов значились тематические постановки, которые отличались идейной направленностью и характером исполнения. Хореографические композиции «Времена года», «Два жока», «Революционный этюд», «За мир и дружбу», «Чуляндра» расширили список балетмейстерских работ.

Уровень подготовки артистов самодеятельных коллективов был поднят на такой уровень, который позволял исполнять хореографические композиции любой сложности. Будь то классическое pasdetrois из балета Чайковского «Лебединое озеро», «Умиравший лебедь» Сен-Санса или вальс на музыку Шопена, сложные многонациональные сюиты или сюжетные юмористические картинки, в которых блистательно раскрывались образы и характеры героев «Соакра ши трей нурорь» и «Жок де глумэ».

Уделяя внимание созданию разнообразных тематических номеров, небольших хореографических миниатюр и развернутых сюжетных композиций, большой энтузиаст, вдумчивый интерпретатор и пропагандист народной хореографии старался привить участникам коллективов любовь к танцевальному искусству и воспитать в них культуру сценического исполнения. Выступления творческих коллективов на различных сценических площадках Молдавской республики, участие в народных праздниках песни и танца, в концертных программах для рабочих и тружеников села, представляли собой подлинно народные праздники, демонстрирующие успехи руководителя и участников коллективов.

Незабываемым событием для коллектива Бендерского Дома культуры под руководством Б. Решетникова стало участие в 1960 году в Декаде молдавского искусства и



литературы в Москве. Вместе с артистами оперного и балетного театра, режиссерами и художниками, поэтами и писателями, ансамблями народного танца республики, участники художественной самодеятельности знакомили трудящихся столицы с ярким и жизнерадостным творчеством молдавского народа. Навсегда осталось в их памяти посещение урока классического танца, которое вела сама Галина Уланова, и заключительный концерт, состоявшийся на сцене Большого театра СССР.

Для того чтобы артисты смогли передать эмоциональную составляющую танца, а зритель в полной мере насладиться красотой исполнения, руководителю необходимо было постоянно находиться в творческом поиске. Много материала было прочитано, изучено и воплощено на практике. Много интересных идей в будущем нашли свое отражение на различных сценических площадках нашей страны и далеко за её пределами.

Новые концертные программы с большим успехом представлялись на проводимых фестивалях, смотрах и конкурсах. Творческий союз Заслуженного деятеля искусств МССР Бориса Решетникова и Отличного работника культуры СССР, виртуозного скрипача Ангела Банчик стал результатом постоянного стремления к развитию и совершенствованию. Многокрасочная палитра единого звучания создавала новое музыкально-танцевальное представление, впечатляющее эмоциональной и пластической выразительностью.

Повышение идейного уровня репертуара стало еще одним шагом по пути раскрытия нового образа средствами хореографического искусства. Композиции: «Бун е винул гюргюлиу», «Хора маре», «Комсомольцы 20-х годов» были отмечены высокой оценкой жюри Республиканских фестивалей. Домом народного творчества в Риге был издан сборник молдавских танцев, поставленных Борисом Решетниковым: «Сырба фетелор», «Молдовеняска», «Хай, ла хорэ», «Хора маре», «Жок де глуме».

Постоянное стремление к творчеству приводило к успешной реализации задуманного. Выезжая с фольклорными экспедициями на фестивали и праздники, проходившие в Молдавии, Румынии и России, Борис Решетников собирал и изучал музыкально-танцевальный материал.

Поистине неиссякаемым народным источником, наполненным характерными для нашего края музыкой, песнями и танцами, были молдавские свадьбы. Наблюдая за тем, как танцуют хору старики, Борис Николаевич старался разгадать секрет исполнения молдавских танцев. Темперамент молдавского народа, его жизнерадостность и оптимизм, прекрасное сочетание музыки и танца – вот что являлось основой в создании



хореографических произведений, отличающихся чистотой стиля и красотой формы [2]. Борис Николаевич был автором постановок различных хореографических форм. Но только большие формы, по его мнению, могли в полной мере донести до зрительской аудитории то, что хотелось выразить балетмейстеру.

После выступления ансамбля в 1970 году на II Всесоюзном фестивале ансамблей народного танца «Дружба народов» в Кишиневе, кандидат философских наук, профессор, Заслуженный деятель искусств России В. И. Уральская писала: «Пожалуй, особенно приятно, что наряду со старыми испытанными молдавскими танцами появляются новые образцы. Рядом с традиционной и известной хорой соседствовал малоизвестный «Кыте трей порниця ла жок» – очень красивый танец, который прекрасно исполнил молдавский коллектив.

За подготовку коллективов к Всесоюзному смотру художественной самодеятельности на ВДНХ СССР в городе Москва и Московской области в 1972 году Борис Решетников был награжден грамотой, подписанной Министром культуры СССР Е. А. Фурцевой, за большую организаторскую работу в развитии самодеятельного искусства и обеспечение успешного выступления коллективов художественной самодеятельности.

Отдавая всего себя любимой профессии, Борис Решетников не только работал над созданием хореографических композиций и воспитанием будущих артистов, но и с 1972 года входил в состав методического совета. Вместе с грамотными специалистами он оказывал практическую и теоретическую помощь по дальнейшей активной работе руководителей, по организации учебно-творческой деятельности хореографических коллективов. Консультируя, проводя методические встречи и открытые занятия, он поддерживал и направлял работу начинающих хореографов.

Творческая энергия и удивительная работоспособность Бориса Решетникова вывела ансамбли в разряд лучших самодеятельных коллективов республики, которые получили право выступать на главных сценах нашей страны и быть посланцами советского многонационального искусства за рубежом.

Достоинство представляя молдавскую культуру на международных фестивалях народного танца в Чехословакии «Стражница – 72», на смотре в Болгарии «Квитна Тракия» (1973), в Польше (1974, 1975), участники ансамблей знакомили зрителей с искрометными танцами своего края.

Подтверждением высокого профессионализма и таланта балетмейстера Бориса Решетникова стало предложение руководителя государственного ансамбля народного



танца МССР Заслуженного деятеля искусств МССР Владимира Курбета пополнить постановками «Хора маре», «Сус-опинка» и «Сэрбэторяска» репертуар ансамбля.

За творческими победами коллективов можно было наблюдать, читая газеты того периода. Печатные периодические издания «Молодежь Молдавии» и «Днестровская правда» гордо освещали их победы и достижения. В 1977 году особой гордостью для Б. Решетникова стало вручение свидетельства о записи в Книгу Почета народных талантов Молдавской ССР.

Составляя концертные программы для очередных гастрольных поездок, руководитель ансамбля всегда старался включать в них новые танцы. Борис Решетников за столько лет работы в ансамбле утвердил в коллективе дух творчества, воспитал в его участниках любовь и преданность хореографическому искусству.

Он считал свой характер несносным, трудным, но, как часто, это понятие «трудный характер» означает преданность делу и требовательность к другим, и, прежде всего, к себе. Это постоянный поиск рисунка танца, средств обогащения его всё новыми и новыми красочными народными мотивами, забота о том, чтобы ярче засверкал в нём национальный колорит

Благодаря Б.Решетникову стали замечательными мастерами танца В.Буга, В. Чоткэ, Л.Чебручан, М.Постован, Заслуженная артистка МССР В.Дикуссар, солистка Государственного ансамбля народного танца «Жок» Л.Опря, Отличные работники культуры МССР Н.Абросимова, Н.Брынзан, А.Каранфил, Н.Титика, Г.Токарева и многие другие, которые раскрывали перед зрителями идейную глубину хореографического произведения, создавали яркие образы и добивались сценической правды зрелища [3].

Он ушёл, оставив светлую память и большое количество преданных ему учеников. Трудно сказать, сколько поколений он воспитал, скольким привил любовь к танцу и сколько занимавшихся под его руководством посвятили свою жизнь хореографическому искусству, став профессиональными танцовщиками, руководителями танцевальных коллективов, педагогами и репетиторами хореографических студий. Их бесчисленное множество.

#### **Литература:**

1. Дымченко Н.В. Виорике – 50. - Тирасполь: 1995. - 44 с.
2. Королева Э.А. Хореографическое искусство Молдавии. - Кишинев: Штиинца, 1970. - 187 с.
3. Барбиер Н. Машина времени для "Переницы" // Новое время . - 2017. - 28.12. - Ст. 7



Гусейнов Вагиф Фазил оглы

Воспитатель учебного курса, г. Ставрополь

ФГКОУ «Ставропольское ПКУ»

## ПРОБЛЕМЫ ПАТРИОТИЧЕСКОГО ВОСПИТАНИЯ В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ

Аннотация: В современном мире человек сталкивается с огромным потоком информации, который поступает через различные цифровые каналы. В условиях глобализации и активного распространения информационных технологий патриотическое воспитание становится сложной задачей, требующей новых подходов и решений.

*Ключевые слова: патриотическое воспитание, глобальная цифровизация, патриотическая информация, борьба с дезинформацией.*

*Key words: patriotic education, global digitalization, patriotic information, fight against disinformation.*

В современном мире человек сталкивается с огромным потоком информации, который поступает через различные цифровые каналы.

В условиях глобализации и активного распространения информационных технологий патриотическое воспитание становится сложной задачей, требующей новых подходов и решений. Цифровые технологии предоставляют пользователю доступ к неограниченному количеству информационных ресурсов, содержащих в том числе недостоверные сведения о его Родине, её истории, культуре и достижениях. Вместе с тем, возникает риск искажения или представления неполной информации, что может привести к формированию ложных представлений о патриотизме и национальных ценностях.

Прежде всего основной проблемой является избыток информации, приводящий к сложности её фильтрации и соответственно усвоению потребителем недостоверных сведений, формирующих образ родного государства не соответствующий действительности. [1] В таких условиях создается возможность манипуляции сознанием молодёжи через неконтролируемые потоки информации через многочисленные цифровые каналы.



Складывающаяся ситуация осложняется еще и тем, что наблюдается общее снижение интереса к традиционным формам патриотического воспитания с учетом высокой конкурентности досуговых и развлекательных ресурсов, а также непроверенной «фейковой» информации. Все это неизбежно приводит к утрате связи между поколениями и разрыву в передаче культурных ценностей.

В целях исключения негативных тенденций и повышения эффективности патриотического воспитания в современных условиях необходимо учитывать ряд значимых аспектов. Во-первых, следует актуализировать существующие образовательные программы по истории и культуре страны, дополняя и наполняя их органичным для восприятия воспитанником материалом, в знакомых ему виде и формах. Достижение указанной модернизации возможно через включение в образовательный материал интерактивных и увлекательных форматов обучения и воспитания (игры, квесты, видеоматериалы).

Не менее значимым фактором представляется активное использование социальных сетей и цифровых платформ для распространения патриотической информации с целью создания конкурентных условий в борьбе с дезинформацией и деструктивным контентом. Актуальным является привлечение юных пользователей к общественно полезной деятельности

на указанных ресурсах, так как наиболее гармоничные для восприятия материалы создаются их же потребителями. [2]

При этом, нельзя преуменьшать роль педагогов и родителей в процессе патриотического воспитания и в современных условиях. Помимо контрольных и кураторских функций старшее поколение способно вносить традиционный вклад в воспитание, в том числе в новых реалиях.

Прежде всего родители и педагоги могут показывать личный пример уважительного отношения к истории и культуре, критического мышления в отношении непроверенной или ложной информации, побуждая тем самым воспитанников к самостоятельному анализу усвоенного в различных источниках.

Также актуальны дискуссии и обсуждения с молодыми людьми текущих событий и тенденций. Вместе с тем, не следует прибегать к напористости в отстаивании своей точки зрения. Наиболее эффективным представляется аргументированная полемика с приведением конкретных исторических примеров и фактов.



В условиях многонационального характера общественно-политического строя нашего государства необходимо поддерживать интерес к изучению национальных традиций и обычаев, уделяя достаточное внимание каждому воспитаннику, истории его народности и семьи. В рассматриваемом аспекте эффективным является привлечение семьи как института социализации, формирующего основные культурные и морально-нравственные ценности.

В качестве действенного способа вовлечения молодежи в самостоятельное изучение национальных традиций представляется их включение в социальные проекты, направленные на сохранение исторической памяти, ее популяризацию и доступность для каждого. Современное поколение способно эффективно использовать имеющиеся у них навыки пользования интернет-ресурсами для создания цифровых платформ и программного обеспечения, которое может органично использоваться их сверстниками.

Таким образом, патриотическое воспитание в условиях глобальной цифровизации непременно требует новых подходов и методов, учитывающих специфику цифрового поколения. Для успешного формирования патриотических качеств необходимо активно использовать цифровые инструменты и ресурсы, разрабатывать образовательные программы и вовлекать молодёжь в процесс создания соответствующих ресурсов и материалов.

#### **Литература:**

1. Мохов В. П. Патриотизм и политика памяти в условиях глобализации // Технологос. 2019. №3. URL: <https://cyberleninka.ru/article/n/patriotizm-i-politika-pamyati-v-usloviyah-globalizatsii> (дата обращения: 10.02.2025).

2. Федосов А. Ю. Гражданско-патриотическое воспитание школьников в условиях цифровой трансформации образования // Нижегородское образование. 2021. №2. URL: <https://cyberleninka.ru/article/n/grazhdansko-patrioticheskoe-vozpitanie-shkolnikov-v-usloviyah-tsifrovoy-transformatsii-obrazovaniya> (дата обращения: 10.02.2025).