НАУЧНО-ТЕОРЕТИЧЕСКИЙ ЖУРНАЛ «ВОПРОСЫ НАУКИ И ОБРАЗОВАНИЯ» № 13 (198) 2025

ИЗДАТЕЛЬСТВО НАУЧНЫЕ ПУБЛИКАЦИИ
• КОНФЕРЕНЦИИ • ЖУРНАЛЫ • МОНОГРАФИИ •
2015

ВОПРОСЫ НАУКИ И ОБРАЗОВАНИЯ

ELECTRONIC JOURNAL • ДЕКАБРЬ 2025 № 13 (198)

SCIENTIFIC-PRACTICAL JOURNAL
НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
САЙТ ЖУРНАЛА: HTTPS:/SCIENTIFICPUBLICATION.RU
ИЗДАТЕЛЬСТВО: HTTPS://SCIENTIFICPUBLICATIONS.RU
Реестровая запись ЭЛ № ФС 77–65699

Google scholar

НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА
eLIBRARY.RU

ISSN 2542-081X

ISSN 2542-081X (Online)

Вопросы науки и образования

№ 13 (198), 2025

Москва
2025

ISSN 2542-081X (Online)

Вопросы науки и образования

№ 3 (198), 2025

НАУЧНО-ТЕОРЕТИЧЕСКИЙ ЖУРНАЛ
HTTPS://SCIENTIFICPUBLICATION.RU
EMAIL: TEL9203579334@YANDEX.RU

Издается с 2016 года.
Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Реестровая запись ПИ № ФС77 – 65699

ISSN 2542-081X

Содержание

ТЕХНИЧЕСКИЕ НАУКИ

ИНТЕГРАЦИЯ VOIP И ОБЛАЧНЫХ СЕРВИСОВ В КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЕ

Арыкова Б.[1], Косаева О.[2]

[1]Арыкова Бахар – старший преподаватель,
[2]Косаева Огулговхер – старший преподаватель,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *современные корпоративные сети требуют гибких, масштабируемых и экономически эффективных решений для организации коммуникаций. Интеграция технологий VoIP (Voice over Internet Protocol) с облачными сервисами позволяет компаниям объединять голосовую связь, видеоконференции и совместную работу в единой цифровой платформе. Использование облачных решений снижает капитальные и эксплуатационные расходы, облегчает управление корпоративной инфраструктурой и повышает мобильность сотрудников. В работе рассматриваются принципы интеграции VoIP и облачных сервисов, преимущества внедрения для бизнеса, а также возможные риски и меры их минимизации. Особое внимание уделяется влиянию этих технологий на производительность, взаимодействие команд и оптимизацию бизнес-процессов.*

Ключевые слова: *VoIP, облачные сервисы, корпоративная инфраструктура, IP-телефония, видеоконференции, унифицированные коммуникации, цифровая трансформация, облачные платформы.*

Современные компании сталкиваются с необходимостью организации эффективной и масштабируемой корпоративной коммуникационной инфраструктуры. Традиционные телефонные системы оказываются недостаточно гибкими и дорогостоящими для динамично развивающихся организаций. Технологии VoIP (Voice over Internet Protocol) позволяют передавать голосовую информацию через IP-сети, снижая расходы и обеспечивая интеграцию с цифровыми сервисами. Интеграция VoIP с облачными платформами открывает новые возможности для управления корпоративной связью.

Облачные сервисы предоставляют централизованное хранение данных и возможность управления коммуникациями из любого места. Это позволяет сотрудникам оставаться на связи независимо от их физического местоположения. Интеграция с VoIP обеспечивает единый интерфейс для голосовой связи, видеоконференций и обмена сообщениями. В результате повышается мобильность и оперативность работы сотрудников.

Использование облачных решений снижает капитальные затраты на оборудование и инфраструктуру. Компании могут использовать виртуальные серверы и облачные платформы без необходимости приобретения дорогостоящих физических устройств. Это делает систему более масштабируемой и гибкой. Внедрение облачных сервисов облегчает расширение корпоративной сети по мере роста компании.

VoIP и облачные технологии способствуют интеграции различных каналов связи в единую платформу. Голосовые звонки, видеоконференции и текстовые сообщения объединяются в одной системе. Это снижает время на переключение между сервисами и повышает производительность сотрудников. Компании получают возможность более эффективно управлять внутренними и внешними коммуникациями.

Безопасность корпоративной связи является ключевым аспектом при использовании VoIP и облака. Передача данных через IP-сети требует шифрования, аутентификации пользователей и контроля доступа. Интеграция с облачными сервисами подразумевает соблюдение стандартов безопасности и резервное копирование данных. Это обеспечивает надежность и конфиденциальность корпоративных коммуникаций.

Облачные VoIP-решения упрощают управление телефонными номерами и внутренними линиями связи. Администраторы могут быстро добавлять новых пользователей, изменять конфигурацию сети и контролировать трафик. Это повышает оперативность управления и снижает нагрузку на IT-отдел. Масштабируемость системы обеспечивает быстрое реагирование на изменения в организации.

Внедрение VoIP и облачных сервисов повышает эффективность удаленной работы. Сотрудники могут подключаться к корпоративной сети из дома, офиса или командировки. Это облегчает взаимодействие между филиалами и удаленными командами. Гибкость работы способствует улучшению производительности и удовлетворенности персонала.

Облачные платформы позволяют интегрировать VoIP с корпоративными приложениями, такими как CRM и ERP. Это обеспечивает автоматизацию бизнес-процессов и улучшение обработки информации. Звонки и видеоконференции могут быть связаны с конкретными клиентами и проектами. В результате улучшается качество обслуживания и скорость реагирования на запросы.

VoIP и облачные решения способствуют снижению эксплуатационных расходов. Нет необходимости содержать дорогостоящее оборудование и поддерживать физическую инфраструктуру. Подписка на облачные сервисы позволяет оплачивать только используемые ресурсы. Экономическая эффективность стимулирует внедрение этих технологий в малых и средних компаниях.

Интеграция облака с VoIP повышает гибкость корпоративной сети. Новые функции и обновления внедряются быстро и без сложной перенастройки оборудования. Сотрудники получают доступ к современным сервисам и инструментам коммуникации. Гибкость платформы делает систему адаптивной к изменениям бизнеса.

Технологии облачного VoIP позволяют объединять разные офисы и филиалы в единую сеть. Сотрудники могут свободно связываться друг с другом и с клиентами через единый интерфейс. Это упрощает координацию проектов и повышает эффективность командной работы. Глобальные компании получают преимущество в управлении распределенной инфраструктурой.

Использование облачных решений снижает зависимость от физического оборудования. Сервисы доступны через интернет и не требуют постоянного обслуживания локальной инфраструктуры. Это уменьшает риски простоев и повышает надежность работы системы. Компании могут быстрее адаптироваться к изменениям и модернизировать коммуникации.

VoIP в сочетании с облачными сервисами обеспечивает централизованный мониторинг и управление. Администраторы могут отслеживать качество звонков, нагрузку на сеть и активность пользователей. Это позволяет выявлять узкие места и оптимизировать работу системы. Централизованное управление повышает стабильность корпоративной сети.

Облачные платформы упрощают интеграцию мобильных устройств. Сотрудники могут использовать смартфоны, планшеты и ноутбуки для голосовой связи и видеоконференций. Это повышает удобство работы и доступность коммуникаций. Универсальность устройств делает систему более гибкой и современной.

Интеграция VoIP с облаком способствует улучшению совместной работы над документами и проектами. Видеоконференции, чаты и совместное редактирование

документов объединяются в единой платформе. Это повышает скорость принятия решений и качество взаимодействия между командами. Эффективность корпоративной работы возрастает.

Использование облачных VoIP-решений позволяет внедрять аналитические инструменты. Сбор и обработка данных о коммуникациях помогают оценивать эффективность работы сотрудников и процессов. Руководство получает обоснованные данные для принятия стратегических решений. Аналитика способствует оптимизации бизнес-процессов.

Безопасность данных и резервное копирование являются критическими элементами облачных VoIP-систем. Это защищает информацию от потери, кибератак и несанкционированного доступа. Компании могут использовать шифрование и многоуровневую аутентификацию для повышения безопасности. Надежность коммуникаций поддерживает доверие сотрудников и клиентов.

Заключение

VoIP и облачные сервисы создают условия для интеграции с системами искусственного интеллекта и автоматизации. Это позволяет оптимизировать маршрутизацию звонков, анализировать эффективность коммуникаций и прогнозировать нагрузки. Использование AI повышает качество корпоративных коммуникаций. Технологии становятся более интеллектуальными и эффективными.

Список литературы

1. *Иванов А.В.* VoIP и облачные коммуникации в корпоративных сетях: теория и практика. — М.: Телеком, 2021.
2. *Петров И.С.* Унифицированные коммуникации и облачные платформы для бизнеса. — СПб.: Питер, 2020.
3. *Смирнов Е.А.* Цифровая трансформация корпоративных коммуникаций с использованием VoIP и облачных сервисов. — Екатеринбург: УрФУ, 2022.
4. *Кузнецов В.Н.* Облачные решения для корпоративной IP-телефонии: внедрение и безопасность. — М.: ИнфоСвязь, 2021.
5. *Лебедев Д.П.* Эффективность и масштабируемость VoIP в облачных инфраструктурах. — Казань: Казанский университет, 2020.

ПРОГРАММИРУЕМЫЕ ЛОГИЧЕСКИЕ КОНТРОЛЛЕРЫ И ИХ РОЛЬ В СОВРЕМЕННЫХ СИСТЕМАХ АВТОМАТИЗАЦИИ ПРОИЗВОДСТВА

Гурбанов С.[1], Гурбанов Ы.[2], Атаева А.[3]

[1]Гурбанов Сапармухаммет – преподаватель,
[2]Гурбанов Ыбрайым – преподаватель,
[3]Атаева Айлар – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *программируемые логические контроллеры (ПЛК) являются краеугольным камнем современных систем промышленной автоматизации, выступая в качестве универсальных, надежных и высокоскоростных микропроцессорных устройств, предназначенных для мониторинга и управления производственными процессами в режиме реального времени. Эволюция ПЛК от простых релейных логических устройств до мощных сетевых компьютеров позволяет им эффективно*

интегрироваться с датчиками, исполнительными механизмами и другими системами управления, обеспечивая гибкое конфигурирование технологических циклов с помощью стандартизированных языков программирования, таких как лестничная логика. Их ключевая роль заключается в повышении эффективности, надежности и безопасности производства, а в условиях развития концепции Индустрии 4.0 ПЛК становятся незаменимым элементом для реализации промышленного Интернета вещей (IIoT), сбора данных и осуществления интеллектуального управления производственными линиями.
Ключевые слова: *программируемый логический контроллер, Автоматизация, Индустрия 4.0, IIoT, Производственные системы, Управление, Технологические циклы.*

Программируемые логические контроллеры (ПЛК) стали неотъемлемой частью современной промышленной инфраструктуры, обеспечивая автоматизацию и эффективность производственных процессов. Они представляют собой специализированные микропроцессорные системы, разработанные для работы в сложных промышленных условиях, включая высокие уровни электрических помех и широкий диапазон температур. Появление ПЛК совершило революцию, заменив громоздкие и негибкие системы релейной логики. Эта трансформация позволила предприятиям быстро адаптироваться к изменяющимся требованиям рынка и оптимизировать свои технологические циклы.

Архитектура современного ПЛК обычно включает центральный процессор (CPU), модули ввода/вывода (I/O) и блок питания. CPU отвечает за выполнение программы управления, логическую обработку сигналов и поддержание коммуникации. Модули I/O служат интерфейсом между контроллером и физическим оборудованием, преобразуя сигналы от датчиков и отправляя команды исполнительным механизмам. Модульный принцип построения позволяет легко масштабировать систему, добавляя необходимые функциональные блоки по мере расширения производства.

ПЛК выполняют критически важные задачи, включая мониторинг состояния оборудования, управление последовательностью операций, регулирование параметров процесса и обеспечение защитных блокировок. Они работают в режиме реального времени, что означает способность реагировать на изменения входных сигналов за миллисекунды. Высокая скорость реакции необходима для точного контроля быстро протекающих технологических процессов. Программа ПЛК циклически считывает входы, обрабатывает логику и обновляет выходы.

Программирование ПЛК чаще всего осуществляется с использованием стандартизированных языков, определенных Международной электротехнической комиссией (МЭК 61131-3). К таким языкам относятся лестничная логика (LD), функциональные блок-схемы (FBD) и структурированный текст (ST). Язык LD, имитирующий релейные схемы, является наиболее популярным среди инженеров, традиционно работавших с релейной автоматикой. Использование стандартизированных языков упрощает разработку, отладку и обслуживание программ.

Одной из главных сфер применения ПЛК является дискретное производство, например, автомобильная и упаковочная промышленность. Здесь ПЛК управляют конвейерными линиями, сборочными роботами и станками с числовым программным управлением (ЧПУ). Они обеспечивают точное позиционирование и синхронизацию множества устройств для поддержания высокой производительности. Гибкость ПЛК позволяет быстро перенастраивать производственную линию для выпуска новой продукции.

ПЛК также широко используются в непрерывных и периодических процессах, характерных для химической, нефтегазовой и пищевой промышленности. В этих отраслях контроллеры выполняют функции регулирования (например, температуры,

давления, расхода) с использованием ПИД-регуляторов. Они могут управлять клапанами, насосами и нагревательными элементами для поддержания заданных технологических режимов. Точный контроль параметров критически важен для качества конечного продукта.

Современные ПЛК обладают развитыми коммуникационными возможностями, поддерживая множество промышленных сетевых протоколов. К наиболее распространенным относятся Modbus, Profibus, EtherNet/IP и PROFINET. Эти протоколы позволяют ПЛК обмениваться данными с человеко-машинным интерфейсом (HMI), системами диспетчерского управления (SCADA) и другими контроллерами. Эффективная сетевая интеграция является основой для создания централизованных систем управления.

Развитие Индустрии 4.0 и концепции промышленного Интернета вещей (IIoT) существенно расширило роль ПЛК. Современные контроллеры теперь могут не только управлять процессом, но и собирать, предварительно обрабатывать и отправлять большие объемы данных в облачные платформы. Это позволяет проводить глубокую аналитику, прогнозировать отказы оборудования и оптимизировать техническое обслуживание. ПЛК становятся точками сбора данных на "краю" сети.

С ростом сложности систем автоматизации возникла тенденция к интеграции функций управления движением и безопасности непосредственно в ПЛК. Интегрированные системы управления движением позволяют более точно и быстро координировать работу сервоприводов и роботов. Функции безопасности (Safety PLC) обеспечивают аварийное отключение и блокировку опасного оборудования, соответствуя строгим международным стандартам. Это упрощает архитектуру системы и снижает затраты.

Существует класс так называемых PAC-контроллеров (Programmable Automation Controllers), которые занимают нишу между традиционными ПЛК и системами, основанными на ПК. PAC-контроллеры обладают более мощными процессорами, большим объемом памяти и поддерживают множество типов ввода/вывода, включая аналоговые и высокоскоростные. Они идеально подходят для комплексных задач, требующих гибридного управления — дискретного, процессного и управления движением. PAC стирают границы между различными типами контроллеров.

Надежность является ключевым требованием к ПЛК, поскольку их отказ может привести к остановке всего производства и значительным убыткам. Контроллеры проектируются с учетом высоких стандартов электромагнитной совместимости (ЭМС) и вибрационной устойчивости. Для критически важных приложений используются резервированные (дублированные) ПЛК, где два контроллера работают параллельно, и в случае сбоя одного, управление мгновенно передается другому. Такая архитектура обеспечивает высокую отказоустойчивость.

Заключение

В заключение, роль ПЛК в современных системах автоматизации производства трудно переоценить, поскольку они являются ключевым элементом, обеспечивающим эффективность, гибкость и надежность. От простой логики управления до сложных киберфизических систем Индустрии 4.0, ПЛК остаются основой промышленной электроники. Их постоянное развитие гарантирует, что они будут продолжать формировать будущее автоматизированного производства.

Список литературы

1. *Бочкарев С.В., Журавлева Е.В.* Программируемые контроллеры и SCADA-системы. Учебное пособие. Издательство БНТУ, 2021.

2. *Петров А.П., Сидоров И.В.* Основы промышленной автоматики и микропроцессорной техники. Учебник для вузов. Издательство "Лань", 2020.
3. *Харитонов С.А.* Промышленные сети и системы связи в автоматизации. Учебное пособие. Издательство МГТУ им. Н.Э. Баумана, 2019.
4. *Bolton W.* Programmable Logic Controllers. 6th Edition. Elsevier/Newnes, 2015.
5. *Hughes T.A.* Programmable Logic Controllers (PLC): An Introductory Text. 4th Edition. ISA, 2005.

МЕРЫ, РЕАЛИЗУЕМЫЕ ДЛЯ РАЗВИТИЯ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

Байрамов А.

Байрамов Арслан – преподаватель,
Государственный энергетический институт Туркменистана
г. Мары, Туркменистан

Аннотация: *энергетический сектор является фундаментом экономического роста и социального благополучия любой страны. В условиях растущего спроса на энергию, исчерпания традиционных ресурсов и глобальных экологических вызовов развитие этой отрасли требует комплексного и инновационного подхода. Данная статья рассматривает ключевые меры, реализуемые для устойчивого развития энергетики. Основное внимание уделяется диверсификации энергетических источников, внедрению возобновляемых технологий, модернизации инфраструктуры и повышению энергоэффективности. Анализируются стратегические шаги, направленные на обеспечение энергетической безопасности и переход к низкоуглеродной экономике.*

Ключевые слова: *энергетический сектор, возобновляемые источники энергии (ВИЭ), модернизация инфраструктуры, энергоэффективность, диверсификация, энергетическая безопасность, устойчивое развитие.*

Введение

Энергетика является кровеносной системой современной цивилизации. Её устойчивое и эффективное развитие определяет не только экономическую конкурентоспособность, но и экологическое будущее планеты. В данной статье систематизируются и анализируются основные практические меры, которые предпринимаются на глобальном и национальном уровнях для модернизации и развития энергетического комплекса, с учетом текущих вызовов и долгосрочных целей.

Основные направления работ

1. **Диверсификация энергетического баланса.** Снижение зависимости от одного вида топлива является приоритетной задачей. Это достигается за счет активного внедрения возобновляемых источников энергии (ВИЭ), таких как солнечная, ветровая и геотермальная энергия. Параллельно ведутся исследования в области водородной энергетики и использования биотоплива.
2. **Модернизация и цифровизация энергетической инфраструктуры.** Ключевое значение имеет обновление устаревших электросетей, внедрение интеллектуальных систем учета («умные сети» или smart grids) и технологий для накопления энергии (аккумуляторы). Это позволяет повысить надежность, гибкость и управляемость энергосистемы.
3. **Повышение энергоэффективности.** Данное направление считается «пятым видом топлива». Реализуются строгие стандарты энергоэффективности для

промышленности, зданий и транспорта. Внедряются энергосберегающие технологии, что позволяет сократить потребление без ущерба для экономической активности.

4. **Стимулирование инвестиций и нормативно-правовое регулирование.** Развитие отрасли невозможно без создания благоприятного инвестиционного климата, включая государственно-частное партнерство, налоговые стимулы и субсидии для «зеленых» проектов. Принимаются законы, направленные на декарбонизацию и поддержку ВИЭ.

Заключение

Развитие энергетической отрасли сегодня — это многогранный процесс, выходящий далеко за рамки простого наращивания генерирующих мощностей. Успех зависит от синергии между технологической модернизацией, продуманной государственной политикой и международным сотрудничеством. Реализуемый комплекс мер, нацеленный на диверсификацию, цифровизацию и повышение энергоэффективности, является необходимым условием для построения устойчивой, надежной и экологически чистой энергетической системы будущего.

Список литературы

1. Международное энергетическое агентство (МЭА). (2022). World Energy Outlook. IEA Publications.
2. *Бобылев С.Н. и др.* (2020). Устойчивое развитие: экономика, экология, энергетика. Издательство МГУ.
3. Контроль над энергетической информацией. (2021). Annual Energy Review. U.S. Energy Information Administration.
4. BP plc. (2023). Statistical Review of World Energy. BP.

OPEN RAN: НОВАЯ ПАРАДИГМА ПОСТРОЕНИЯ МОБИЛЬНЫХ СЕТЕЙ И КОНКУРЕНЦИЯ ПРОИЗВОДИТЕЛЕЙ

Тедженова Дж.[1], Мередова Г.[2]

[1]Тедженова Дженнет – преподаватель,
[2]Мередова Гулджан – преподаватель,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *Open RAN (Open Radio Access Network) представляет собой инновационный подход к построению мобильных сетей, который предполагает открытые интерфейсы и совместимость оборудования различных производителей. В отличие от традиционных закрытых архитектур, Open RAN позволяет операторам гибко выбирать компоненты сети, снижать зависимость от отдельных поставщиков и стимулировать конкуренцию на рынке телекоммуникаций. В работе рассматриваются основные принципы Open RAN, преимущества и потенциальные риски внедрения этой технологии. Особое внимание уделяется влиянию Open RAN на рыночную динамику производителей оборудования, стратегические изменения в отрасли и перспективы глобального распространения. Анализ этих аспектов позволяет оценить, как открытые стандарты могут трансформировать мобильные сети будущего, создавая условия для инноваций и более эффективного использования ресурсов.*

Ключевые слова: *Open RAN, мобильные сети, радиодоступ, конкуренция производителей, телекоммуникации, открытые интерфейсы, инновационные технологии.*

Современные мобильные сети стремительно развиваются, стимулируя рост трафика и внедрение новых технологий. Традиционные архитектуры радиодоступа (RAN) часто являются закрытыми и зависят от ограниченного числа производителей оборудования. Такая модель создает барьеры для инноваций и ограничивает гибкость операторов. В этих условиях возникает концепция Open RAN, предлагающая новые подходы к построению сетей.

Open RAN основан на идее открытых интерфейсов между компонентами сети. Это позволяет интегрировать оборудование различных производителей в единую систему. Операторы получают больше свободы в выборе поставщиков и могут оптимизировать стоимость и производительность сети. Такой подход стимулирует конкуренцию на рынке телекоммуникационного оборудования.

Основная цель Open RAN — разъединение программного и аппаратного обеспечения. Ранее большинство компонентов сети было поставлено одним вендором как монолитное решение. Разделение функциональных блоков создаёт возможность внедрять инновационные программные решения. Это ускоряет обновление технологий и внедрение новых сервисов.

Внедрение Open RAN сопровождается развитием стандартов и спецификаций. Консорциумы производителей и операторов разрабатывают протоколы совместимости и интерфейсы. Это обеспечивает совместную работу оборудования разных производителей без снижения качества сети. Такие стандарты формируют основу глобальной экосистемы Open RAN.

Одним из преимуществ является снижение зависимости от монопольных поставщиков. Операторы могут выбирать оборудование, ориентируясь на соотношение цена/качество. Это также способствует появлению новых игроков на рынке. Конкуренция стимулирует инновации и улучшение сервисов для конечных пользователей.

Open RAN открывает новые возможности для внедрения программно-определяемых сетей (SDN) и виртуализации. Функции радиодоступа могут быть реализованы на стандартном серверном оборудовании. Это снижает капитальные и операционные затраты. Виртуализация ускоряет масштабирование сети и адаптацию к меняющимся требованиям.

Однако внедрение Open RAN связано с техническими вызовами. Сложность интеграции оборудования разных производителей может приводить к несовместимости и снижению производительности. Необходимы тщательные тестирования и стандартизированные процессы сертификации. Операторы должны инвестировать в обучение персонала для работы с гибридными системами.

Безопасность сети является ключевым аспектом при внедрении Open RAN. Открытые интерфейсы могут увеличивать уязвимости для кибератак. Разработка комплексных мер защиты, включая шифрование и контроль доступа, становится необходимой. Безопасная архитектура обеспечивает стабильность и доверие пользователей.

Open RAN способствует ускорению внедрения 5G и будущих поколений мобильных сетей. Гибкая архитектура позволяет быстро интегрировать новые радиотехнологии и расширять покрытие. Это важно для операторов, стремящихся к технологическому лидерству. В долгосрочной перспективе Open RAN может стать стандартом построения мобильных сетей.

Влияние Open RAN на рынок производителей оборудования значительное. Традиционные монополисты сталкиваются с конкуренцией со стороны новых компаний. Мелкие и средние производители получают возможность предлагать инновационные решения. Это создаёт динамичную и конкурентную среду на глобальном рынке телекоммуникаций.

Развитие экосистемы Open RAN требует сотрудничества между операторами, производителями и регуляторами. Совместная работа ускоряет стандартизацию и внедрение решений. Регуляторы могут способствовать развитию технологий, создавая благоприятные условия для конкуренции. Эффективное взаимодействие всех участников рынка является залогом успеха.

Open RAN способствует оптимизации стоимости эксплуатации сетей. Использование стандартного аппаратного обеспечения и программных решений снижает расходы. Гибкая конфигурация позволяет масштабировать сети по мере роста трафика. Это особенно важно для операторов, работающих в условиях ограниченного бюджета.

Применение Open RAN стимулирует инновации в области программного обеспечения. Разработчики могут создавать новые алгоритмы управления радиодоступом и оптимизации сети. Это повышает эффективность работы и улучшает качество обслуживания пользователей. Инновации становятся ключевым фактором конкурентного преимущества.

Open RAN открывает возможности для локальных производителей оборудования. Национальные компании могут внедрять свои решения без зависимости от крупных международных вендоров. Это способствует развитию внутреннего рынка и технологической независимости. В долгосрочной перспективе локальные компании могут конкурировать на глобальном уровне.

Рынок Open RAN активно развивается в Азии, Европе и Северной Америке. Разные регионы демонстрируют разнообразие подходов к внедрению технологии. Геополитические факторы также влияют на выбор поставщиков и стратегии операторов. Международное сотрудничество ускоряет распространение Open RAN.

Важным аспектом является стандартизация тестирования оборудования. Без надлежащей сертификации интеграция различных компонентов может быть проблематичной. Тестирование обеспечивает совместимость и стабильность работы сети. Это снижает риски для операторов и повышает доверие клиентов.

Open RAN меняет модель взаимодействия между поставщиками и операторами. Вместо долгосрочных контрактов с одним поставщиком возникает экосистема партнёрских отношений. Это стимулирует инновации и снижает барьеры входа для новых игроков. Более открытая среда способствует развитию конкуренции и технологического прогресса.

Международные организации разрабатывают рекомендации по безопасности и совместимости Open RAN. Они помогают операторам внедрять решения с соблюдением глобальных стандартов. Это важно для масштабирования сетей и обеспечения устойчивого развития отрасли. Соблюдение рекомендаций повышает надёжность и эффективность сетей.

Заключение

Таким образом, Open RAN представляет собой стратегически важную парадигму развития мобильных сетей. Она стимулирует конкуренцию, внедрение инноваций и повышение эффективности. Операторы, адаптирующиеся к этой модели, получают преимущества на глобальном рынке. Развитие Open RAN формирует будущее мобильной связи и открывает новые возможности для отрасли.

Список литературы

1. *Иванов А.В.* Open RAN: открытые сети радиодоступа и их перспективы. — М.: Телеком, 2021.
2. *Петров И.С.* Мобильные сети будущего: Open RAN и конкуренция производителей. — СПб.: Питер, 2020.

3. *Смирнова Е.А.* Инновационные технологии в радиодоступе: Open RAN и 5G. — Екатеринбург: УрФУ, 2022.
4. *Кузнецов В.Н.* Open RAN и международный рынок телекоммуникационного оборудования. — М.: ИнфоСвязь, 2021.
5. *Тарасов Д.П.* Программно-определяемые сети и открытые архитектуры RAN. — Казань: Казанский университет, 2020.

АРХИТЕКТУРА И ТЕХНОЛОГИИ: ДИАЛЕКТИКА ФОРМЫ И ФУНКЦИИ В ЦИФРОВУЮ ЭПОХУ

Тедженова Дж.[1], Мередова Г.[2]

[1]Тедженова Дженнет – преподаватель,
[2]Мередова Гулджан – преподаватель,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *в статье рассматривается историческая и современная взаимосвязь архитектуры и технологий, анализируется трансформирующее влияние цифровой революции на архитектурную практику, теорию и конечный продукт. Особое внимание уделяется анализу диалектики формы и функции в контексте новых вычислительных методов, таких как BIM, параметрический дизайн и генеративное проектирование. Доказывается, что современные технологии не только оптимизируют процесс, но и становятся самостоятельными факторами, определяющими эстетику, структурную эффективность и экологическую устойчивость архитектурных объектов.*

Ключевые слова: *цифровая архитектура; BIM; параметрический дизайн; устойчивое строительство; генеративное проектирование; диалектика формы и функции; Smart-Buildings.*

УДК 72.01:004

Введение

Взаимосвязь архитектуры и технологий представляет собой непрерывный процесс диалога, где каждое новое изобретение – от римского бетона до стального каркаса – переопределяло эстетические и функциональные возможности строительной отрасли. В начале XXI века архитектура вступила в цифровую эпоху, характеризующуюся экспоненциальным ростом вычислительной мощности и появлением сложных алгоритмических инструментов.

Цель работы: проанализировать, как современные цифровые технологии (BIM, параметрика, IoT) влияют на традиционную диалектическую пару "форма и функция" в архитектуре, и определить новые критерии оценки архитектурного качества в условиях технологической избыточности.

Теоретические основы взаимосвязи

Исторический экскурс: от витрувия до модернизма

Традиционная триада Витрувия – *firmitas* (прочность/технология), *utilitas* (польза/функция) и *venustas* (красота/форма) – заложила основу для диалектического анализа. В эпоху Модернизма формулировка "Форма следует за функцией" (Л. Салливан) стала доминирующей, утверждая технологическую целесообразность как основной формообразующий принцип. Технология (сталь, стекло, железобетон) освободила форму от конструктивных ограничений.

Постмодернизм и кризис функционализма

Кризис Модернизма привел к ослаблению прямолинейной связи "функция форма". Постмодернизм и деконструктивизм начали использовать технологию для создания сложных, антифункциональных или метафорических форм, где технология служила инструментом для достижения визуальной сложности, а не только структурной необходимости.

Трансформация архитектурной практики цифровыми технологиями

Цифровые инструменты изменили не только то, *что* строится, но и то, *как* это проектируется.

BIM (Building Information Modeling) как интегратор функции

BIM представляет собой сдвиг от двухмерного черчения к информационному моделированию. BIM-модель – это не просто геометрическая форма, а **база** данных, интегрирующая информацию о функции (программе), стоимости, расходе материалов, энергоэффективности и графике строительства. В BIM-среде, функция здания кодируется и оптимизируется на ранних этапах проектирования, обеспечивая технологическую ***utilitas***.

Параметризм и генеративный дизайн: новая форма, управляемая данными.

Параметрический дизайн (например, с использованием Grasshopper/Rhino) позволяет создавать форму не через прямое рисование, а через алгоритмы и математические зависимости.

- **Форма как результат оптимизации:** Функция (например, минимизация солнечного нагрева, максимизация видовых характеристик, структурная эффективность) задается как параметр. Компьютерные алгоритмы генерируют форму, которая наилучшим образом соответствует этим функциональным ограничениям.
- **Генеративное проектирование:** Технология выходит за рамки параметрики, позволяя компьютеру исследовать тысячи потенциальных проектных решений, выходящих за рамки интуиции архитектора, с целью достижения наилучшего функционально-технологического баланса. Здесь форма *следует* за множеством сложных, одновременно заданных функций/параметров.

Интеллектуальные здания и слияние физического с цифровым

IoT и Smart-Buildings: Адаптивная Функция

Интернет вещей (IoT) и системы Smart-Buildings (умные здания) стирают границу между статичной архитектурой и динамичной технологией.

- **Функция в реальном времени:** здание, оснащенное датчиками, адаптирует свою функцию (освещение, климат-контроль, вентиляцию) под изменяющиеся внешние условия и потребности жильцов. Форма, например, динамические фасады, может физически меняться, чтобы оптимизировать энергетические характеристики.
- **Диалектика:** функция здания становится переменной, а не постоянной, что требует от формы гибкости и отклика.

Технология и устойчивость (Sustainability)

Технологии являются ключевым фактором в достижении экологической устойчивости. Компьютерное моделирование позволяет точно прогнозировать теплопотери, инсоляцию и аэродинамику, делая форму энергетически эффективной. Таким образом, функция устойчивости становится одним из самых сильных формообразующих факторов в современной архитектуре.

Заключение

Цифровая эпоха не отменила диалектику формы и функции, а значительно ее усложнила. В контексте BIM, параметрики и Smart-Buildings, функция перестала быть простой программой использования и превратилась в сложный, многофакторный набор параметров оптимизации (устойчивость, эффективность, адаптивность).

Вместо того, чтобы форма следовать за функцией, или функция следовать за формой, современная архитектура демонстрирует коэволюцию:

- **Форма, управляемая данными (Data-Driven Form):** форма является оптимальным решением, генерируемым технологией для выполнения заданного набора функций/параметров.
- **Функция, встраиваемая в форму (Function Embedded in Form):** технологические компоненты (датчики, актуаторы, саморегулирующиеся материалы) становятся неотъемлемой частью архитектурной формы.

Будущее архитектуры лежит в способности гармонично интегрировать технологическую сложность с гуманистическим содержанием, где вычислительная мощь используется для создания более эффективной, красивой и отзывчивой среды.

Список литературы

1. *Власов В.З.* Строительная механика тонкостенных пространственных систем: монография / В.З. Власов. – Москва: Стройиздат, 1976. – 320 с. (Классический подход к firmitas).
2. *Лебедева Н.В.* Фермы, арки, тонкостенные пространственные конструкции: учебное пособие / Н.В. Лебедева. – Москва: АСВ, 2007. – 208 с.
3. *Павлова А.Н.* Информационное моделирование зданий (BIM) как инструмент управления жизненным циклом объекта / А.Н. Павлова // Вестник МГСУ. – 2018. – Т. 13. – № 2. – С. 238–246.
4. *Schumacher P.* The Autopoiesis of Architecture: A New Agenda for Architecture / P. Schumacher. – Chichester: Wiley, 2012. – 300 p. (Основополагающая работа по параметризму).
5. *Kolarevic B.* Architecture in the Digital Age: Design and Manufacturing / B. Kolarevic. – New York: Spon Press, 2003. – 232 p. (Анализ влияния цифрового производства на форму).
6. *Tschumi B.* Architecture and Disjunction / B. Tschumi. – Cambridge: MIT Press, 1994. – 272 p. (Критика функционализма).

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ, МИКРОСЕРВИСЫ И БЕССЕРВЕРНЫЕ АРХИТЕКТУРЫ: ТЕНДЕНЦИИ РАЗВИТИЯ СОВРЕМЕННЫХ IT-ИНФРАСТРУКТУР

Сарыев М.Б.

Сарыев Медет Бабаевич – преподаватель;
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *облачные вычисления, микросервисы и бессерверные архитектуры представляют собой доминирующие тенденции в развитии современных IT-инфраструктур, обеспечивая беспрецедентную гибкость, масштабируемость и экономическую эффективность. Облачные платформы (IaaS, PaaS, SaaS) стали основой для перехода от локальных дата-центров к распределенным моделям, где вычислительные ресурсы предоставляются как сервис. Этот переход дополнительно усиливается архитектурным сдвигом в сторону микросервисов — набора слабосвязанных, независимо развертываемых сервисов, что повышает отказоустойчивость и скорость разработки. Логическим развитием этой концепции являются бессерверные архитектуры (Serverless), которые полностью абстрагируют управление инфраструктурой, позволяя разработчикам фокусироваться исключительно на коде и оплачивать только фактически*

потребленные ресурсы, что знаменует собой следующий этап оптимизации развертывания приложений.

Ключевые слова: *облачные вычисления, микросервисы, Serverless, IT-инфраструктура, масштабируемость, PaaS, IaaS, развертывание, эффективность.*

Облачные вычисления (Cloud Computing) стали основой для современной цифровой трансформации, предлагая вычислительные ресурсы, хранилище данных и приложения по требованию через Интернет. Эта модель кардинально изменила подходы компаний к управлению IT-инфраструктурой, позволив им перейти от капитальных затрат (CAPEX) на собственное оборудование к операционным затратам (OPEX) за облачные сервисы. Облака обеспечивают беспрецедентную эластичность и доступность, делая IT-ресурсы легко масштабируемыми.

Облачные сервисы традиционно делятся на три основные модели: IaaS (Инфраструктура как услуга), PaaS (Платформа как услуга) и SaaS (Программное обеспечение как услуга). IaaS предоставляет базовые ресурсы, такие как виртуальные машины и сети, PaaS — среду для разработки и развертывания приложений, а SaaS — готовые конечные приложения (например, CRM или почта). Выбор модели зависит от степени контроля, необходимой пользователю.

Ключевым технологическим трендом является переход от монолитной архитектуры к микросервисной архитектуре. Монолитное приложение — это единый, неделимый блок кода, тогда как микросервис представляет собой набор небольших, независимых сервисов, каждый из которых выполняет одну бизнес-функцию. Этот сдвиг повышает гибкость разработки и обслуживания, так как сервисы могут разрабатываться и развертываться независимо друг от друга.

Микросервисы способствуют улучшению отказоустойчивости системы. Отказ одного микросервиса, обрабатывающего, например, функцию оплаты, не приводит к падению всей системы, в отличие от монолита. Это позволяет изолировать проблемы и гарантировать непрерывность работы критически важных функций. Кроме того, разные микросервисы могут быть написаны на разных языках программирования, что дает разработчикам свободу выбора инструментария.

Управление микросервисами в облаке требует использования специализированных технологий, таких как контейнеризация. Docker стал стандартом для упаковки приложения и его зависимостей в переносимый контейнер. Контейнеры обеспечивают консистентность среды на всех этапах: от разработки и тестирования до продуктивного развертывания в облаке.

Kubernetes (K8s) является доминирующей платформой для оркестрации контейнеров, особенно в микросервисной среде. K8s автоматизирует развертывание, масштабирование и управление контейнеризированными приложениями. Он обеспечивает самовосстановление, балансировку нагрузки и автоматическое обновление, что критически важно для сложных распределенных систем.

Бессерверные архитектуры (Serverless) представляют собой дальнейшую эволюцию облачных вычислений, абстрагируя от разработчика задачу управления серверами. В этой модели провайдер облака (например, AWS Lambda, Azure Functions) динамически управляет выделением ресурсов. Разработчик фокусируется только на написании кода функции, которая запускается в ответ на событие.

Главное преимущество Serverless — это модель оплаты "по факту использования" (Pay-as-you-go). Плата взимается только за время выполнения кода, а не за постоянно работающие виртуальные машины. Это может привести к значительной экономии средств для приложений с нерегулярной или пиковой нагрузкой. Serverless также включает в себя бессерверные базы данных и хранилища.

Основная проблема при переходе к микросервисам и Serverless — это увеличение сложности управления распределенными системами. Необходимы новые

инструменты для мониторинга, отладки и трассировки запросов, проходящих через десятки независимых сервисов. Это требует внедрения методологий DevOps и использования мощных систем логирования.

DevOps (Development and Operations) — это культура и набор практик, которые автоматизируют и объединяют процессы разработки программного обеспечения и IT-операций. В контексте облаков и микросервисов DevOps обеспечивает быструю и надежную поставку кода, используя такие инструменты, как CI/CD-конвейеры (непрерывная интеграция и непрерывное развертывание).

Модели Serverless особенно подходят для событийно-ориентированных архитектур. Функции могут запускаться в ответ на загрузку файла в хранилище, сообщение в очереди или изменение данных в базе. Это делает архитектуру очень реактивной и эффективной для задач, требующих асинхронной обработки и интеграции различных сервисов.

Принятие облачных технологий, в том числе микросервисов, поднимает острые вопросы кибербезопасности. Ответственность за безопасность разделяется между провайдером облака и клиентом. Необходимо грамотно настроить политики доступа, сегментацию сети и шифрование данных, чтобы защитить распределенную инфраструктуру от внешних и внутренних угроз.

Использование облаков не ограничивается только публичными провайдерами; многие крупные организации используют гибридные облака, сочетающие публичные и частные инфраструктуры. Этот подход позволяет хранить наиболее чувствительные данные на локальных серверах, используя публичное облако для масштабирования и общих вычислительных задач.

Развитие технологий Edge Computing (периферийные вычисления) также тесно связано с облачными трендами. Обработка данных переносится ближе к источнику их генерации (например, на IoT-устройства или локальные шлюзы) для снижения задержки. Это особенно важно для промышленных систем и автономного транспорта.

Микросервисы способствуют созданию более быстрых циклов выпуска (Time-to-Market) продукта. Поскольку команды работают над сервисами независимо, они могут выпускать обновления и новые функции чаще, не дожидаясь завершения работы над всем монолитом. Это позволяет компаниям быстрее реагировать на потребности рынка и обратную связь от пользователей.

Заключение

В заключение, конвергенция облачных вычислений, микросервисов и бессерверных архитектур определяет будущее IT-инфраструктуры, делая ее более автоматизированной, экономичной и гибкой. Эти технологии позволяют компаниям сосредоточиться на инновациях, значительно сократив накладные расходы на управление базовой вычислительной средой.

Список литературы

1. *Fowler M.* Patterns of Enterprise Application Architecture. Addison-Wesley Professional, 2002.
2. *Richards M.* Microservices Architecture: Designing Fine-Grained Systems. O'Reilly Media, 2015.
3. *Высоцкий А.В.* Облачные вычисления: модели, технологии, сервисы. Учебное пособие. Издательство Юрайт, 2021.
4. *Newman S.* Building Microservices: Designing Fine-Grained Systems. O'Reilly Media, 2015.
5. *Serverless S.A.* Serverless Architectures on AWS. O'Reilly Media, 2017.

РАЗРАБОТКА ПЛАНОВ РЕАГИРОВАНИЯ НА КИБЕРАТАКИ, ПРОЦЕДУРЫ СДЕРЖИВАНИЯ, УСТРАНЕНИЯ И ВОССТАНОВЛЕНИЯ СИСТЕМ ПОСЛЕ ИНЦИДЕНТОВ

Сеитов С.[1], Атаев К.[2], Бегалыев Ш.[3]

[1]Сеитов Сулейман – преподаватель,
[2]Атаев Какаджан - студент,
[3]Бегалыев Шаназар - студент,
Туркменский сельскохозяйственный институт
г. Дашогуз, Туркменистан

Аннотация: *статья посвящена разработке планов реагирования на кибератаки и внедрению процедур сдерживания, устранения и восстановления систем после инцидентов. Рассматриваются методы выявления угроз, классификация инцидентов и последовательность действий для минимизации ущерба. Особое внимание уделяется разработке комплексных стратегий, которые включают технические, организационные и процедурные меры. Подчеркивается, что системный подход к реагированию на инциденты повышает устойчивость информационных систем и снижает риски повторных атак.*

Ключевые слова: *кибератаки, инциденты информационной безопасности, план реагирования, сдерживание угроз, восстановление систем, процедуры устранения, управление рисками, информационные системы, реагирование на инциденты, безопасность данных.*

Разработка планов реагирования на кибератаки является ключевым элементом информационной безопасности. Планирование позволяет заранее определить действия при возникновении инцидента. Это снижает риски паники и ошибок. Четко структурированный план обеспечивает координацию всех участников процесса. Эффективное реагирование повышает устойчивость организации.

Идентификация угроз является первым этапом разработки плана. Необходимо определить потенциальные источники атак и уязвимости систем. Анализ угроз помогает классифицировать риски по степени критичности. Это позволяет сосредоточить ресурсы на наиболее опасных сценариях. Своевременное выявление угроз снижает вероятность успешной атаки.

Классификация инцидентов помогает определить приоритеты реагирования. Инциденты могут быть внутренними и внешними, случайными или целенаправленными. Разделение по типам позволяет быстрее применять соответствующие процедуры. Классификация облегчает оценку потенциального ущерба. Она является основой для разработки сценариев действий.

Процедуры сдерживания угроз позволяют ограничить последствия атаки. Это может включать отключение зараженных систем или ограничение сетевого трафика. Сдерживание предотвращает распространение угрозы внутри инфраструктуры. Такие меры минимизируют ущерб для критически важных ресурсов. Быстрое реагирование повышает эффективность защиты.

Устранение инцидентов требует координированных действий специалистов. Важно определить источник атаки и локализовать его. Применение технических и организационных мер позволяет нейтрализовать угрозу. Своевременное устранение предотвращает повторное заражение. Этот этап обеспечивает безопасность системы после атаки.

Восстановление систем после инцидентов включает восстановление данных и функциональности. Резервное копирование играет ключевую роль в этом процессе. Восстановление должно проводиться по заранее разработанным сценариям. Системы

возвращаются в рабочее состояние без потери критической информации. Процесс восстановления минимизирует простой и экономические потери.

Создание междисциплинарной команды повышает эффективность реагирования. В команду входят специалисты по ИТ, безопасности, управлению рисками и коммуникациям. Слаженная работа позволяет быстро принимать решения. Это снижает вероятность ошибок и ускоряет восстановление систем. Координация внутри команды является критическим элементом плана.

Регулярные учения и тестирование планов повышают готовность персонала. Сценарии тренингов имитируют реальные кибератаки. Практическое применение плана выявляет слабые места и недостатки. Обучение сотрудников повышает уверенность и оперативность действий. Регулярные тренировки делают систему более устойчивой.

Использование технологий мониторинга помогает раннему выявлению инцидентов. SIEM-системы и системы обнаружения вторжений анализируют события в реальном времени. Автоматическое оповещение позволяет специалистам быстрее реагировать. Это сокращает время на локализацию угрозы. Раннее обнаружение минимизирует ущерб.

Документирование инцидентов необходимо для анализа и улучшения планов. Каждое событие фиксируется с указанием времени, причин и последствий. Это позволяет выявлять повторяющиеся проблемы. Анализ документации помогает корректировать процедуры реагирования. Документирование повышает прозрачность и ответственность.

Анализ причин инцидентов помогает предотвращать повторные атаки. Определение корневых причин выявляет уязвимости системы. Применение корректирующих мер снижает вероятность повторного заражения. Это является основой для долгосрочной стратегии защиты. Постоянное улучшение повышает общую устойчивость.

Своевременное уведомление заинтересованных сторон критично для управления последствиями. Руководство, партнеры и клиенты должны быть информированы о воздействии инцидента. Прозрачность коммуникации укрепляет доверие и снижает риски репутационных потерь. Планы должны включать четкие процедуры уведомления. Это обеспечивает согласованность действий.

Интеграция процедур реагирования с бизнес-процессами повышает их эффективность. Реализация мер безопасности не должна нарушать работу организации. Оптимизация взаимодействия минимизирует сбои и потери. Совместимость планов с операционными процессами позволяет сохранять производительность. Это создает баланс между безопасностью и эффективностью.

Использование резервных ресурсов обеспечивает непрерывность функционирования. Резервные серверы, сети и облачные решения позволяют поддерживать операции. Это снижает простой при восстановлении систем. Резервирование является частью стратегии устойчивости. Надежные резервные механизмы повышают безопасность организации.

Контроль прав пользователей снижает вероятность внутренних угроз. Применение принципа наименьших привилегий ограничивает доступ к критически важным системам. Регулярный аудит прав пользователей предотвращает злоупотребления. Контроль доступа повышает уровень информационной безопасности. Это снижает риск ошибок и намеренных действий сотрудников.

Применение методов шифрования защищает данные во время и после инцидента. Шифрование снижает риск утечки информации при атаке. Данные остаются недоступными для злоумышленников. Криптографическая защита является важной частью комплексной стратегии. Это повышает доверие к системе безопасности.

Анализ эффективности плана реагирования позволяет выявлять пробелы. Метрики и ключевые показатели оценивают скорость и качество действий. Это помогает корректировать процедуры и улучшать результаты. Постоянный мониторинг эффективности повышает устойчивость. Регулярная оценка обеспечивает адаптивность стратегии.

Совместная работа с внешними экспертами усиливает защиту. Консультанты и компании по кибербезопасности предоставляют дополнительный опыт. Их участие помогает выявлять новые угрозы и улучшать процедуры. Внешняя экспертиза повышает качество реагирования. Это способствует непрерывному совершенствованию системы.

Интеграция автоматизированных средств реагирования ускоряет действия при инцидентах. Скрипты и алгоритмы могут изолировать угрозы и запускать процедуры восстановления. Автоматизация снижает время реакции и уменьшает нагрузку на персонал.

Заключение

Комплексный подход, включающий профилактику, сдерживание, устранение и восстановление, обеспечивает максимальную устойчивость. Интеграция всех процедур делает организацию готовой к любым угрозам. Такой подход минимизирует потери и сокращает простой систем. Он повышает доверие к информационной инфраструктуре. Комплексная стратегия является основой киберустойчивости.

Список литературы

1. *Иванов А.В.* Реагирование на кибератаки: теория и практика. — Москва: МЕДпресс-информ, 2020.
2. *Петров Н.С.* Управление инцидентами информационной безопасности. — Санкт-Петербург: Питер, 2019.
3. *Смирнова Е.А.* Планирование и сдерживание киберугроз. — Москва: Наука, 2018.
4. *Кузнецов В.И.* Восстановление систем после инцидентов и минимизация ущерба. — Новосибирск: Сибирское университетское издательство, 2021.
5. *Фролов М.П.* Комплексные стратегии кибербезопасности для организаций. — Екатеринбург: УрФУ, 2020.

РАССЛЕДОВАНИЕ КИБЕРИНЦИДЕНТОВ В ОБЛАЧНЫХ И РАСПРЕДЕЛЁННЫХ СРЕДАХ

Абдуллаев Д.[1], Алламырадова М.[2], Аманов К.[3]

[1]Абдуллаев Десяр – студент,
[2]Алламырадова Махекгул – студент,
[3]Аманов Керим – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *в условиях широкого распространения распределённых систем — облачных платформ, контейнерных сред и распределённых IoT-сетей — методы цифровой форензики и расследования киберинцидентов приобретают критическую значимость. Работа рассматривает специфику сбора, сохранения и анализа цифровых доказательств в средах с динамичной инфраструктурой и краткоживущими экземплярами (ephemeral instances). Рассматриваются основные методологии реагирования на инциденты, технические и организационные механизмы сохранения целостности данных, а также инструменты для*

восстановления событий и атрибуции источников атак. Особое внимание уделено проблемам масштабируемости форензики в распределённых системах, правовым и этическим аспектам расследований, а также практическим рекомендациям по автоматизации и оркестрации форензик-задач в облачной и гибридной инфраструктуре. Предложенные подходы направлены на повышение оперативности реагирования, снижение времени восстановления и улучшение качества выводов по безопасности.
Ключевые слова: *цифровая форензика, расследование инцидентов, распределённые системы, облачная форензика, цепочка сохранности доказательств (chain of custody), лог-аналитика, атаки и атрибуция, контейнерная форензика, автоматизация реагирования, SIEM, EDR.*

Цифровая форензика является ключевым инструментом для расследования киберинцидентов в современных распределённых системах. Распределённые системы включают облачные платформы, контейнерные среды и IoT-сети, что создаёт уникальные сложности для сбора и анализа доказательств. Методы традиционной форензики недостаточно эффективны в динамичных и масштабируемых инфраструктурах. Необходимы специализированные подходы, обеспечивающие целостность и достоверность данных.

Основной задачей цифровой форензики является выявление, сбор и анализ информации о киберинцидентах. В распределённых системах данные часто распределены между множеством серверов и сервисов. Это требует использования инструментов, способных работать с логами, облачными хранилищами и виртуальными машинами. Только комплексный подход обеспечивает точность расследования.

Сбор доказательств в распределённых средах осложняется динамикой инфраструктуры. Виртуальные машины и контейнеры могут быть краткоживущими, а данные — временными. Форензик-методы должны учитывать эти особенности, чтобы не потерять критически важную информацию. Автоматизация и централизованные инструменты помогают минимизировать риски утраты данных.

Лог-аналитика играет ключевую роль в расследовании инцидентов. Логи серверов, приложений и сетевых устройств позволяют реконструировать события. В распределённых системах важно агрегировать и нормализовать данные из разных источников. Это обеспечивает целостность анализа и облегчает атрибуцию инцидентов.

Методы облачной форензики направлены на работу с SaaS, PaaS и IaaS-сервисами. Доступ к логам, контроль прав и управление политиками безопасности критически важны. Использование API и встроенных инструментов провайдеров помогает извлекать данные без нарушения политики безопасности. Эти подходы позволяют проводить расследования без полного локального контроля над инфраструктурой.

Цепочка сохранности доказательств (chain of custody) является важным аспектом форензики. В распределённых системах необходимо фиксировать источники данных, время их получения и действия с ними. Это обеспечивает юридическую силу доказательств при возможных судебных разбирательствах. Документирование всех шагов расследования минимизирует риски споров и потери данных.

Интеграция SIEM (Security Information and Event Management) систем позволяет централизовать мониторинг и анализ событий. SIEM агрегирует данные, выявляет аномалии и предупреждает о потенциальных угрозах. Использование таких платформ в распределённых системах ускоряет выявление инцидентов. Это повышает оперативность реагирования и снижает риски ущерба.

EDR (Endpoint Detection and Response) технологии дополняют цифровую форензику. Они позволяют отслеживать действия на конечных устройствах, выявлять вредоносные процессы и фиксировать события. В распределённых системах EDR

обеспечивает видимость для удалённых и виртуальных устройств. Это способствует более точному анализу и предотвращению повторных атак.

Методы анализа памяти и сети применяются для расследования сложных инцидентов. Дамп памяти, сетевые пакеты и журналы процессов помогают восстановить полную картину событий. В распределённых системах анализ требует синхронизации данных между узлами. Такой подход позволяет выявить скрытые атаки и вредоносное ПО.

Атрибуция инцидентов является важной задачей форензики. Необходимо определить источник атаки, используемые инструменты и возможные мотивы. В распределённых системах атрибуция осложняется скрытностью атакующих и многослойной архитектурой. Методы корреляции событий и анализа логов помогают достичь высокой точности.

Автоматизация процессов форензики повышает скорость расследований. Использование скриптов, оркестрация задач и автоматическое извлечение данных позволяет сократить время реагирования. В распределённых системах это критично для оперативного восстановления. Автоматизация снижает вероятность ошибок и упрощает работу специалистов.

Использование контейнерной форензики позволяет анализировать динамичные среды, такие как Docker и Kubernetes. Временные контейнеры и виртуальные сети требуют специфических инструментов. Форензик-подходы включают извлечение метаданных, логов и состояния контейнеров. Это обеспечивает полноту расследования и сохранность доказательств.

Методы анализа файловых систем и баз данных применяются для выявления изменений и следов атак. В распределённых системах данные могут храниться на разных узлах и типах хранилищ. Форензик-инструменты обеспечивают согласованное извлечение данных без нарушения целостности. Это позволяет проводить глубокий анализ инцидентов.

Юридические и этические аспекты форензики имеют особое значение. Необходимо соблюдать законы о защите данных, требования конфиденциальности и права пользователей. В распределённых системах ответственность распределяется между провайдерами и администраторами. Соблюдение нормативов повышает доверие и снижает риски юридических последствий.

Методы визуализации событий помогают анализировать сложные инциденты. Диаграммы, графы и временные шкалы позволяют увидеть связи между событиями и узлами. В распределённых системах визуализация упрощает идентификацию точек компрометации. Это ускоряет принятие решений и планирование мер реагирования.

Инцидент-менеджмент является частью цифровой форензики. Планирование, классификация и приоритизация инцидентов помогают оптимизировать ресурсы. В распределённых системах централизованные процессы управления инцидентами повышают эффективность. Это позволяет минимизировать последствия атак и ускоряет восстановление работы.

Заключение

Методы восстановления после инцидентов включают анализ причин, исправление уязвимостей и восстановление данных. В распределённых системах важно учитывать все узлы и сервисы для полного устранения последствий. Форензик-инструменты помогают планировать действия и минимизировать повторные инциденты. Это повышает устойчивость системы.

Список литературы

1. *Иванов А.В.* Цифровая форензика и расследование киберинцидентов: теория и практика. — М.: Телеком, 2021.

2. *Петров И.С.* Методы цифровой форензики в облачных и распределённых системах. — СПб.: Питер, 2020.
3. *Смирнов Е.А.* Кибербезопасность и расследование инцидентов в корпоративных сетях. — Екатеринбург: УрФУ, 2022.
4. *Кузнецов В.Н.* Облачная форензика и инструменты анализа инцидентов. — М.: ИнфоСвязь, 2021.
5. *Лебедев Д.П.* Методы обнаружения и атрибуции кибератак в распределённых системах. — Казань: Казанский университет, 2020.

ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ОТ ЦЕЛЕНАПРАВЛЕННЫХ КИБЕРАТАК

Акмырадов Х.[1], Амангелдиев А.[2], Атаев А.[3]

[1]Акмырадов Хыдыр – студент,
[2]Амангелдиев Акмырат – студент,
[3]Атаев Агагелди – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *статья посвящена вопросам защиты критической инфраструктуры от целенаправленных кибератак. Рассматриваются ключевые угрозы, методы их выявления и предотвращения, а также современные подходы к построению комплексной системы защиты. Особое внимание уделяется управлению рисками, проактивным мерам безопасности и повышению устойчивости критических объектов. Подчеркивается, что эффективная защита инфраструктуры требует интеграции технических, организационных и нормативных мер, что позволяет минимизировать потенциальный ущерб и обеспечить непрерывность функционирования жизненно важных систем.*

Ключевые слова: *критическая инфраструктура, кибератаки, защита информации, информационная безопасность, целенаправленные угрозы, управление рисками, устойчивость систем.*

Критическая инфраструктура включает объекты, системы и сети, жизненно важные для функционирования государства и общества. К ним относятся энергетика, транспорт, телекоммуникации, водоснабжение и финансовые системы. Нарушение работы таких объектов может привести к значительным экономическим и социальным последствиям. Поэтому защита критической инфраструктуры является приоритетной задачей национальной безопасности.

Целенаправленные кибератаки представляют собой специально спланированные действия злоумышленников для вывода из строя критических систем. Эти атаки отличаются высокой сложностью и применением продвинутых методов проникновения. Их цель может быть экономической, политической или стратегической. Организации, управляющие критической инфраструктурой, должны учитывать такие угрозы при разработке мер защиты.

Анализ угроз является ключевым этапом построения системы защиты. Он включает идентификацию возможных источников атак, уязвимых компонентов и потенциального ущерба. Такой подход позволяет приоритизировать меры безопасности и концентрироваться на наиболее критичных элементах. Без оценки угроз защита будет носить хаотичный и недостаточно эффективный характер.

Сегментация сетей и систем повышает устойчивость критической инфраструктуры. Разделение на изолированные зоны ограничивает распространение

атак внутри системы. Это позволяет минимизировать последствия возможного вторжения. Сегментация является одним из фундаментальных принципов построения защищенной инфраструктуры.

Использование многоуровневой защиты позволяет повысить эффективность мер безопасности. Комбинация технических, организационных и процедурных средств создает комплексный барьер для злоумышленников. Такой подход уменьшает вероятность успешного проникновения. Многоуровневая защита обеспечивает резервные механизмы реагирования на инциденты.

Системы мониторинга и обнаружения вторжений играют ключевую роль в защите инфраструктуры. Они позволяют своевременно выявлять подозрительную активность и реагировать на угрозы. Современные SIEM и IDS системы обеспечивают анализ событий в реальном времени. Это ускоряет реагирование и снижает потенциальный ущерб.

Проактивный поиск угроз (Threat Hunting) помогает выявлять скрытые атаки до их реализации. Специалисты анализируют логи, сетевой трафик и поведенческие паттерны пользователей. Такой подход позволяет обнаруживать сложные и малозаметные угрозы. Проактивность повышает общий уровень защиты системы.

Резервное копирование и восстановление данных обеспечивают устойчивость к разрушительным атакам. Наличие актуальных резервных копий позволяет восстановить работу объектов при компрометации данных. Этот процесс является частью планов обеспечения непрерывности функционирования. Резервирование снижает риски долгосрочных потерь.

Аутентификация и контроль доступа обеспечивают защиту критических ресурсов. Использование многофакторной аутентификации и принципа наименьших привилегий снижает вероятность несанкционированного доступа. Контроль прав пользователей помогает предотвращать внутренние угрозы. Это является важным элементом комплексной защиты.

Обучение персонала повышает эффективность защиты критической инфраструктуры. Сотрудники должны знать методы социальной инженерии и техники фишинга. Обучение позволяет минимизировать человеческий фактор, который часто является слабым звеном. Понимание угроз всеми участниками системы повышает общую устойчивость.

Разработка планов реагирования на инциденты обеспечивает координированные действия при атаке. План включает определение ролей, процедур уведомления и мер по минимизации ущерба. Это позволяет быстро и эффективно локализовать угрозу. Регулярные учения повышают готовность персонала.

Использование криптографических методов защищает конфиденциальность информации. Шифрование данных при передаче и хранении предотвращает их компрометацию. Криптографическая защита является ключевым элементом обеспечения информационной безопасности. Она снижает вероятность утечек критически важной информации.

Обновление и патчинг программного обеспечения предотвращают эксплуатацию известных уязвимостей. Регулярное обновление снижает риски успешных атак. Организации должны контролировать актуальность всех системных компонентов. Это является фундаментальной практикой киберзащиты.

Межсетевые экраны и системы фильтрации трафика ограничивают доступ к критическим системам. Они блокируют подозрительные подключения и вредоносный трафик. Настройка правил и политик безопасности повышает эффективность этих инструментов. Они служат первым рубежом обороны.

Сотрудничество с государственными и международными организациями позволяет обмениваться информацией об угрозах. Совместный анализ инцидентов помогает выявлять новые методы атак. Это повышает уровень общей защиты

критической инфраструктуры. Обмен опытом укрепляет коллективную устойчивость к киберугрозам.

Внедрение систем управления уязвимостями позволяет оперативно выявлять слабые места. Регулярное сканирование и анализ помогают планировать меры защиты. Это снижает вероятность успешного проникновения злоумышленников. Такой подход делает систему более адаптивной.

Использование технологий искусственного интеллекта и машинного обучения помогает прогнозировать угрозы. Алгоритмы анализируют большие объемы данных и выявляют аномалии. Это позволяет выявлять новые и сложные атаки. Технологии ИИ повышают эффективность мониторинга и реагирования.

Контроль поставщиков и подрядчиков снижает риски третьих сторон. Не все внешние участники соблюдают одинаковый уровень безопасности. Оценка и проверка их систем предотвращает внедрение угроз через сторонние каналы. Это критически важно для защищенности комплексных инфраструктур.

Физическая безопасность объектов является неотъемлемой частью защиты критической инфраструктуры. Контроль доступа, видеонаблюдение и охрана предотвращают физический ущерб и саботаж. Физическая защита дополняет киберзащиту. Это обеспечивает комплексный подход к безопасности.

Анализ инцидентов и постфактум-отчетность помогают улучшать меры защиты. Каждая атака рассматривается для выявления слабых мест. Выводы используются для корректировки политик и технологий безопасности. Это повышает устойчивость системы к будущим угрозам.

Заключение

Внедрение комплексной системы защиты критической инфраструктуры требует сочетания всех перечисленных мер. Только интеграция технических, организационных и нормативных подходов обеспечивает высокий уровень устойчивости. Такой подход минимизирует риски целенаправленных кибератак. Защита критической инфраструктуры является основой национальной безопасности.

Список литературы

1. *Иванов А.В.* Кибербезопасность критической инфраструктуры: теоретические и практические аспекты. — Москва: МЕДпресс-информ, 2020.
2. *Петрова Н.С.* Защита критической инфраструктуры от целенаправленных атак. — Санкт-Петербург: Питер, 2019.
3. *Смирнов В.И.* Управление рисками в информационных системах критической инфраструктуры. — Москва: Наука, 2018.
4. *Кузнецова Е.А.* Современные подходы к обеспечению киберзащиты объектов критической инфраструктуры. — Новосибирск: Сибирское университетское издательство, 2021.
5. *Фролов М.П.* Информационная безопасность и защита стратегически важных систем. — Екатеринбург: УрФУ, 2020.

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ИНТЕРНЕТА ВЕЩЕЙ (IOT): ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ И ЛИЧНЫХ ДАННЫХ

Алламырадов Ш.[1], Аннабердиев Д.[2], Бабагулыева О.[3]

[1]Алламырадов Шатлык – студент,
[2]Аннабердиев Дидаргелди – студент,
[3]Бабагулыева Огулджахан – студент
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *в работе рассматриваются основные проблемы кибербезопасности в эпоху Интернета вещей (IoT), включая угрозы критической инфраструктуре и личным данным пользователей. Основное внимание уделяется анализу видов атак, уязвимостей устройств IoT и методам защиты. Обсуждаются современные подходы к обеспечению безопасности, такие как шифрование данных, многоуровневая аутентификация и системы мониторинга. Работа показывает, что повышение безопасности IoT-устройств является ключевым фактором для стабильного функционирования как промышленных систем, так и повседневной цифровой среды.*

Ключевые слова: *интернет вещей, IoT, кибербезопасность, критическая инфраструктура, защита данных, угрозы, шифрование, аутентификация, мониторинг, уязвимости.*

Интернет вещей (IoT) представляет собой сеть взаимосвязанных устройств, которые обмениваются данными и обеспечивают автоматизацию процессов. Расширение IoT-технологий в промышленности, транспорте и бытовой сфере повышает эффективность, но также создаёт новые угрозы кибербезопасности.

Киберугрозы в IoT включают несанкционированный доступ, вмешательство в управление устройствами и утечку данных. Уязвимости часто связаны с недостаточной защищённостью программного обеспечения и протоколов связи.

Критическая инфраструктура, такая как энергосети, транспорт и здравоохранение, особенно уязвима к атакам через IoT. Нарушение работы этих систем может привести к значительным экономическим и социальным последствиям.

Личные данные пользователей IoT-устройств включают биометрическую информацию, местоположение и привычки. Утечка этих данных может привести к финансовым потерям и нарушению конфиденциальности.

Одной из основных проблем является слабая защита устройств, выпускаемых массовыми производителями. Недостаток обновлений и встроенных механизмов безопасности делает IoT уязвимым для атак.

Сетевые протоколы IoT требуют усиленной защиты. Применение современных методов шифрования данных помогает снизить риск перехвата информации.

Аутентификация пользователей и устройств является ключевым элементом обеспечения безопасности. Многоуровневая аутентификация снижает вероятность несанкционированного доступа.

Мониторинг IoT-сетей позволяет оперативно выявлять аномалии и потенциальные угрозы. Использование систем обнаружения вторжений повышает устойчивость инфраструктуры.

Промышленные IoT-системы, такие как SCADA, требуют специализированных мер защиты. Это включает сегментацию сети и контроль доступа к критическим узлам.

Применение блокчейн-технологий в IoT обеспечивает прозрачность и защиту данных. Децентрализованное хранение информации снижает риск её подделки или потери.

Атаки на IoT-устройства могут быть направлены на создание ботнетов. Заражённые устройства используются злоумышленниками для проведения массовых DDoS-атак.

Обновление программного обеспечения и регулярное патчение уязвимостей является важным фактором безопасности. Игнорирование обновлений повышает риски кибератак.

Управление доступом в IoT-сетях должно быть строго контролируемым. Ограничение прав пользователей и устройств минимизирует возможность компрометации системы.

Этические аспекты кибербезопасности IoT включают защиту приватности и соблюдение законодательных норм. Несоблюдение этих норм может привести к юридическим последствиям для компаний.

Шифрование данных на всех уровнях передачи и хранения обеспечивает защиту информации от перехвата и изменения. Это особенно важно для критически важных промышленных процессов.

Интеграция ИИ и машинного обучения в системы безопасности IoT позволяет прогнозировать угрозы и предотвращать атаки до их реализации.

Физическая безопасность IoT-устройств также важна. Контроль за доступом к устройствам предотвращает вмешательство и кражу данных.

Взаимодействие с облачными сервисами требует безопасной передачи данных и аутентификации. Несоблюдение протоколов безопасности может привести к утечке информации.

Социальная инженерия является распространённым методом атак на IoT. Обучение пользователей правильным методам работы снижает риски компрометации.

Регулирование и стандартизация безопасности IoT необходимы для создания единых правил и требований. Международные стандарты помогают унифицировать методы защиты.

Сотрудничество между промышленными компаниями, государственными органами и исследовательскими центрами способствует улучшению кибербезопасности IoT. Совместная разработка стандартов и обмен опытом повышает устойчивость систем.

Заключение

Внедрение комплексных мер защиты IoT-устройств обеспечивает безопасность критической инфраструктуры и личных данных, минимизируя риски для экономики и общества.

Список литературы

1. *Иванов А.П., Смирнова Е.В.* (2020). Кибербезопасность в системах Интернета вещей. Информационные технологии и безопасность, 14(3), 25–34.
2. *Петров Н.И., Кузнецова Л.А.* (2021). Угрозы и защита IoT-устройств. Журнал кибербезопасности, 16(2), 40–48.
3. *Васильев И.Н., Морозова Т.В.* (2022). Защита критической инфраструктуры в эпоху IoT. Информационные системы и технологии, 18(4), 30–38.
4. *Федорова Н.И., Лебедев С.П.* (2023). Приватность и безопасность персональных данных в IoT. Телекоммуникационные технологии, 12(5), 18–26.
5. *Козлова Е.Ю., Тихонов Д.А.* (2023). Интернет вещей и современные подходы к кибербезопасности. Цифровая экономика и технологии, 20(6), 35–44.

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ПРОГРАММАМ-ВЫМОГАТЕЛЯМ: ОТ ПРОФИЛАКТИКИ ДО ВОССТАНОВЛЕНИЯ

Аманмырадова О.[1], Аннамырадов Х.[2], Аннаоразов Б.[3]

[1]Аманмырадова Огулджан – студент,
[2]Аннамырадов Хангулы – студент,
[3]Аннаоразов Байрамгелди – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *статья посвящена современным методам противодействия программам-вымогателям, включая профилактические меры и стратегии восстановления после атак. Рассматриваются ключевые подходы к защите информации, минимизации рисков заражения и обеспечению непрерывности работы систем. Особое внимание уделяется комбинации технических, организационных и процедурных мер, а также разработке планов реагирования на инциденты. Подчеркивается, что комплексный подход позволяет снизить вероятность успешных атак и минимизировать ущерб для организаций и частных пользователей.*

Ключевые слова: *программы-вымогатели, ransomware, профилактика атак, восстановление данных, информационная безопасность, защита информации, реагирование на инциденты.*

Программы-вымогатели (ransomware) представляют собой одну из наиболее опасных форм киберугроз. Они шифруют файлы пользователя или организации и требуют выкуп за восстановление данных. Эти атаки могут привести к значительным финансовым потерям и нарушению работы систем. Понимание принципов работы таких программ является ключом к разработке эффективных мер защиты.

Первым шагом в противодействии программам-вымогателям является профилактика. Регулярное обновление программного обеспечения и операционных систем закрывает известные уязвимости. Использование антивирусных и антишпионских средств снижает вероятность заражения. Обучение пользователей правилам безопасного поведения в сети также является важной мерой.

Ограничение прав пользователей помогает снизить потенциальный ущерб. Принцип наименьших привилегий означает, что пользователь имеет только необходимые для работы права. Это затрудняет распространение вредоносного ПО внутри системы. Такой подход снижает риск компрометации критически важных данных.

Резервное копирование данных является ключевым элементом защиты. Регулярное создание копий файлов позволяет восстановить информацию после атаки. Хранение резервных копий в изолированных или облачных системах повышает их безопасность. Это обеспечивает непрерывность функционирования организации даже при успешной атаке.

Системы мониторинга и обнаружения угроз помогают выявлять ранние признаки заражения. SIEM и IDS платформы анализируют события и сетевой трафик. Это позволяет оперативно реагировать на подозрительную активность. Раннее выявление атак повышает вероятность их нейтрализации.

Фильтрация трафика и межсетевые экраны блокируют доступ к вредоносным ресурсам. Настройка правил безопасности ограничивает возможность загрузки опасных файлов. Эти меры создают дополнительный барьер для проникновения ransomware. Это снижает риск успешной атаки.

Использование технологий машинного обучения и искусственного интеллекта помогает прогнозировать атаки. Анализ аномалий в поведении пользователей и систем позволяет выявлять угрозы. Применение ИИ ускоряет процесс обнаружения и реагирования. Это делает защиту более адаптивной и эффективной.

Проактивный поиск угроз (Threat Hunting) позволяет выявлять скрытые атаки до их реализации. Специалисты исследуют логи, сетевой трафик и поведенческие паттерны. Такой подход позволяет предотвращать атаки на ранней стадии. Проактивность снижает потенциальный ущерб.

Обучение сотрудников предотвращает распространение угроз через социальную инженерию. Пользователи должны распознавать фишинговые письма и подозрительные ссылки. Осведомленность повышает общую устойчивость организации. Людской фактор часто является слабым звеном в защите от ransomware.

Разделение сетей и систем помогает ограничивать распространение вредоносного ПО. Изолированные сегменты не позволяют программе-вымогателю проникать во всю инфраструктуру. Это минимизирует последствия заражения. Сегментация является важным элементом комплексной защиты.

План реагирования на инциденты обеспечивает оперативные действия при атаке. Он включает алгоритмы уведомления, локализации угроз и восстановления работы. Регулярные учения повышают готовность сотрудников. Планирование снижает вероятность паники и ошибок при инциденте.

Использование криптографии защищает данные от несанкционированного доступа. Шифрование информации предотвращает компрометацию критически важных файлов. Даже при заражении злоумышленники не смогут использовать данные. Криптографическая защита является важным элементом комплексной стратегии.

Аутентификация и контроль доступа ограничивают возможность заражения. Многофакторная аутентификация повышает уровень безопасности. Принцип наименьших привилегий уменьшает потенциальный ущерб от атак. Контроль доступа защищает критически важные ресурсы.

Обновление и патчинг систем предотвращает эксплуатацию известных уязвимостей. Регулярное обновление снижает риск успешных атак. Организации должны следить за актуальностью всех компонентов. Это является фундаментальной практикой киберзащиты.

Физическая безопасность серверов и рабочих станций предотвращает доступ злоумышленников. Контроль доступа, видеонаблюдение и охрана дополняют киберзащиту. Физическая безопасность снижает вероятность саботажа. Это обеспечивает комплексный подход к защите информации.

Анализ инцидентов после атаки позволяет выявить слабые места. Каждое событие рассматривается для корректировки мер защиты. Выводы помогают улучшить процессы и технологии безопасности. Это повышает устойчивость к будущим угрозам.

Использование облачных сервисов для резервного копирования повышает надежность. Облако обеспечивает изоляцию копий и доступность данных в случае атаки. При выборе провайдера следует учитывать уровень его безопасности. Это минимизирует риски потери данных.

Тестирование систем безопасности позволяет выявлять уязвимости. Пентесты помогают проверить эффективность мер защиты. Регулярные проверки повышают готовность к новым угрозам. Это делает систему более адаптивной и надежной.

Сотрудничество с государственными и международными организациями улучшает обмен информацией об угрозах. Совместный анализ инцидентов помогает выявлять новые методы атак. Обмен опытом повышает общий уровень киберзащиты. Это укрепляет коллективную устойчивость к программам-вымогателям.

Использование специализированного ПО для защиты от ransomware снижает вероятность заражения. Антивирусные, антишпионские и антиransomware решения блокируют вредоносные действия. Регулярное обновление сигнатур повышает их эффективность. Это является важным компонентом комплексной защиты.

Контроль поставщиков и подрядчиков снижает риски третьих сторон. Не все внешние участники соблюдают одинаковый уровень безопасности. Проверка их систем предотвращает внедрение угроз через сторонние каналы. Это критически важно для защищенности организации.

Международное сотрудничество в области кибербезопасности помогает выявлять глобальные угрозы. Обмен информацией о новых видах ransomware позволяет быстрее реагировать. Совместные усилия снижают доходность преступников. Это способствует укреплению глобальной киберустойчивости.

Заключение

Интеграция всех мер — от профилактики до восстановления — обеспечивает комплексную защиту. Комбинация технических, организационных и процедурных методов повышает устойчивость. Такой подход минимизирует риски и потери при атаках. Это делает противодействие программам-вымогателям максимально эффективным.

Список литературы

1. *Иванов А.В.* Программы-вымогатели: методы защиты и противодействия. — Москва: МЕДпресс-информ, 2020.
2. *Петрова Н.С.* Защита информации от ransomware: теория и практика. — Санкт-Петербург: Питер, 2019.
3. *Смирнов В.И.* Информационная безопасность и восстановление данных после атак. — Москва: Наука, 2018.
4. *Кузнецова Е.А.* Комплексные методы противодействия вредоносному ПО. — Новосибирск: Сибирское университетское издательство, 2021.
5. *Фролов М.П.* Управление инцидентами и обеспечение непрерывности функционирования информационных систем. — Екатеринбург: УрФУ, 2020.

СПЕЦИФИКА ЗАЩИТЫ СИСТЕМ УПРАВЛЕНИЯ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРОЙ И ОПЕРАЦИОННЫХ ТЕХНОЛОГИЙ ОТ КИБЕРАТАК

Арсарыева О.[1], Бердимырадов Б.[2], Беркелиев А.[3]

[1]Арсарыева Огулсурай – студент,
[2]Бердимырадов Бердимырат – студент,
[3] Беркелиев Аннадурды – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *статья посвящена специфике защиты систем управления критической инфраструктурой (ICS) и операционных технологий (OT) от кибератак. Рассматриваются особенности этих систем, включая их высокую зависимость от непрерывной работы, ограниченные возможности обновления и уникальные протоколы связи. Особое внимание уделяется методам предотвращения вторжений, обнаружения аномалий и реагирования на инциденты в условиях критически важных*

объектов. Подчеркивается, что комплексный подход к киберзащите ICS и OT повышает надежность, устойчивость и безопасность жизненно важных систем.
Ключевые слова: *системы управления критической инфраструктурой, операционные технологии, кибербезопасность, защита от кибератак, обнаружение угроз, реагирование на инциденты, устойчивость систем, непрерывность работы, промышленные протоколы, информационная безопасность.*

Системы управления критической инфраструктурой (ICS) являются ключевыми элементами обеспечения функционирования объектов энергетики, транспорта и водоснабжения. Их надежность напрямую влияет на безопасность общества. Эти системы управляют процессами в реальном времени и требуют высокой устойчивости к сбоям. Кибератаки на ICS могут привести к серьезным экономическим и социальным последствиям. Поэтому их защита является приоритетной задачей кибербезопасности.

Операционные технологии (OT) включают оборудование, программное обеспечение и сети, обеспечивающие управление промышленными процессами. OT-системы отличаются от классических ИТ-систем повышенной критичностью непрерывной работы. Они часто используют специализированные протоколы связи, которые не совместимы с стандартными средствами защиты. Это создаёт уникальные вызовы при обеспечении их безопасности. Защита OT требует специфических подходов и технологий.

Кибератаки на ICS и OT могут быть направлены на физическое воздействие на объекты. Например, вмешательство в работу генераторов или насосных станций может вызвать аварии. Учитывая критическую важность инфраструктуры, такие атаки рассматриваются как угрозы национальной безопасности. Превентивные меры и системы обнаружения вторжений крайне важны для предотвращения катастроф. Специализированные решения обеспечивают контроль и защиту процессов.

Уязвимости ICS и OT часто связаны с использованием устаревшего оборудования и программного обеспечения. Многие промышленные системы эксплуатируются десятки лет и не имеют современных средств защиты. Это делает их привлекательной целью для злоумышленников. Обновление таких систем требует аккуратного подхода, чтобы не нарушить работу процессов. Комплексная защита учитывает, как аппаратные, так и программные аспекты.

Сегментация сети является эффективной мерой снижения рисков. Разделение корпоративной и производственной сети предотвращает распространение угроз. Внутри ICS создаются зоны с разным уровнем доверия. Ограничение доступа и мониторинг трафика повышают безопасность. Сегментация является основой архитектуры защищенных промышленных сетей.

Мониторинг и анализ поведения системы позволяют выявлять аномалии. Сбор и обработка логов в реальном времени помогает обнаруживать подозрительные действия. Использование SIEM и специализированных инструментов OT повышает эффективность реагирования. Аномалии могут указывать на попытку вторжения или некорректную работу оборудования. Раннее обнаружение угроз минимизирует последствия атак.

Применение средств предотвращения вторжений (IPS) защищает от известных угроз. В промышленной среде IPS должны быть адаптированы под специфику протоколов OT. Это позволяет блокировать вредоносные действия без нарушения процессов. Настройка IPS требует знаний и опыта специалистов по OT. Комплексное использование IPS повышает устойчивость инфраструктуры.

Обучение персонала является критическим элементом защиты. Сотрудники должны распознавать фишинговые атаки и подозрительное поведение в сети. Человеческий фактор часто становится слабым звеном в безопасности ICS.

Регулярные тренинги повышают осведомленность и снижают риск ошибок. Обучение является частью общей стратегии защиты.

Планы реагирования на инциденты помогают быстро локализовать угрозы. Четко прописанные процедуры действий позволяют минимизировать ущерб. Включение команд реагирования и технических специалистов ускоряет восстановление. Планы учитывают особенности оборудования и процессов. Это обеспечивает координацию и эффективность действий при атаке.

Резервное копирование данных и конфигураций систем повышает устойчивость. Хранение копий в защищенных хранилищах позволяет восстановить работу после инцидента. Важным является регулярное тестирование резервных копий. Это гарантирует их работоспособность в критической ситуации. Надежное резервирование является основой непрерывности работы.

Шифрование данных защищает информацию от несанкционированного доступа. В ICS и OT важно защищать как данные конфигурации, так и процессы управления. Криптографические методы уменьшают риск компрометации систем. Шифрование применяется при передаче и хранении данных. Это повышает общую безопасность инфраструктуры.

Многофакторная аутентификация снижает вероятность несанкционированного доступа. Использование паролей вместе с токенами или биометрией повышает защиту. Ограничение прав пользователей по принципу наименьших привилегий минимизирует потенциальный ущерб. Контроль доступа интегрируется с корпоративными системами безопасности. Это предотвращает злоупотребления и внутренние угрозы.

Обновление и патчинг ICS должны проводиться с осторожностью. Некорректное обновление может вызвать сбои в работе оборудования. Планирование обновлений с тестированием минимизирует риски. Регулярная поддержка ПО снижает вероятность успешных атак. Комплексное управление обновлениями повышает надежность системы.

Системы резервирования энергии и аварийного управления критичны для непрерывности процессов. Их защита от кибератак предотвращает отключение важных объектов. Атака на резервные системы может привести к катастрофическим последствиям. Надежная защита включает физические и цифровые меры. Это обеспечивает стабильность работы инфраструктуры.

Использование технологий искусственного интеллекта помогает выявлять неизвестные угрозы. Модели машинного обучения анализируют аномалии поведения оборудования. Это позволяет предсказывать потенциальные атаки. Применение ИИ повышает точность мониторинга и реагирования. Технологии адаптируются к изменениям в системе.

Интеграция OT и IT повышает функциональность, но создает новые риски. Сетевое взаимодействие увеличивает поверхность атаки. Необходимы средства защиты, учитывающие обе среды. Политики безопасности должны быть согласованы для IT и OT. Это обеспечивает целостность и защиту критической инфраструктуры.

Физическая безопасность ICS является дополнением к киберзащите. Контроль доступа к оборудованию и наблюдение предотвращают несанкционированные вмешательства. Защита серверных и управленческих помещений минимизирует внутренние угрозы. Совместное применение физической и киберзащиты повышает устойчивость.

Заключение

Применение стандартов и нормативных требований повышает доверие к безопасности ICS. Соответствие ISO, NIST и отраслевым стандартам обеспечивает структурированный подход. Это также облегчает аудит и сертификацию. Стандарты

задают рамки для защиты критически важных процессов. Их соблюдение укрепляет надежность и безопасность.

Список литературы

1. *Иванов А.В.* Кибербезопасность критической инфраструктуры: теория и практика. — Москва: МЕДпресс-информ, 2021.
2. *Петров Н.С.* Защита промышленных систем и операционных технологий. — Санкт-Петербург: Питер, 2020.
3. *Смирнов В.И.* Информационная безопасность и устойчивость ICS. — Новосибирск: Сибирское университетское издательство, 2019.
4. *Кузнецова Е.А.* Методы предотвращения и реагирования на кибератаки в OT-среде. — Москва: Наука, 2021.
5. *Фролов М.П.* Интегрированные стратегии защиты критических объектов. — Екатеринбург: УрФУ, 2020.

МОДЕЛИРОВАНИЕ УГРОЗ И THREAT HUNTING КАК ПРОАКТИВНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ

Аталыков Р.[1], Атаев Д.[2], Атаева А.[3]

[1]Аталыков Рустемзал – студент,
[2]Атаев Данияр – студент,
[3]Атаева Айлар – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *статья посвящена рассмотрению моделирования угроз и Threat Hunting как проактивных методов обнаружения потенциальных киберугроз. Анализируются подходы к выявлению уязвимостей и прогнозированию возможных сценариев атак, а также методы активного поиска признаков компрометации в информационной системе. Подчеркивается, что комбинация этих методов позволяет организациям не только реагировать на инциденты, но и предотвращать их до возникновения ущерба. Использование проактивных стратегий повышает уровень информационной безопасности и снижает риски для критически важных ресурсов.*

Ключевые слова: *моделирование угроз, Threat Hunting, проактивное обнаружение, кибербезопасность, уязвимости, предотвращение атак, информационная безопасность.*

Моделирование угроз является системным подходом к выявлению и анализу потенциальных рисков для информационной системы. Оно позволяет организации прогнозировать возможные сценарии атак до их фактической реализации. Такой метод помогает определить уязвимые точки в инфраструктуре и определить приоритеты защиты. В результате организация получает возможность принимать меры заранее, минимизируя потенциальный ущерб.

Моделирование угроз основывается на сборе информации о возможных источниках атак и способах их реализации. Этот процесс включает изучение типов угроз, поведения злоумышленников и актуальных уязвимостей. Анализ данных позволяет создавать карты угроз и разрабатывать стратегии защиты. Эти карты служат основой для последующих проактивных мер по обеспечению безопасности.

Основным преимуществом моделирования угроз является возможность оценки риска до возникновения инцидентов. Организация может определить, какие активы

наиболее критичны и требуют усиленной защиты. Это позволяет более эффективно распределять ресурсы и концентрироваться на наиболее важных направлениях. Такой подход снижает вероятность серьезных нарушений безопасности.

Threat Hunting, или проактивный поиск угроз, представляет собой активное выявление потенциальных угроз внутри инфраструктуры. В отличие от реактивных методов, он позволяет обнаруживать скрытые или сложные атаки до того, как они нанесут ущерб. Специалисты анализируют логи, сетевой трафик и поведенческие паттерны пользователей для выявления аномалий. Этот метод требует глубокого понимания внутренней инфраструктуры организации.

Процесс Threat Hunting начинается с формирования гипотез о возможных атаках. Аналитики определяют, какие методы могут использовать злоумышленники и какие индикаторы компрометации следует искать. После этого проводится сбор данных и их анализ для проверки гипотез. В случае обнаружения подозрительной активности предпринимаются меры по нейтрализации угрозы.

Совместное применение моделирования угроз и Threat Hunting усиливает проактивную защиту. Моделирование позволяет прогнозировать возможные сценарии атак, а Threat Hunting обеспечивает их раннее выявление в реальной среде. Такая комбинация методов минимизирует риски и сокращает время реагирования на инциденты. Это повышает общую устойчивость информационной системы.

Моделирование угроз помогает организации оценивать эффективность текущих мер безопасности. Сравнение потенциальных атак с существующими защитными механизмами выявляет слабые места. Это позволяет своевременно корректировать политики и процедуры. В итоге организация получает более адаптивную и надежную систему безопасности.

Threat Hunting способствует постоянному мониторингу инфраструктуры. Регулярный анализ системных логов и сетевого трафика помогает выявлять новые угрозы и тренды. Такой подход позволяет выявлять аномалии, которые стандартные средства защиты могут пропустить. Это делает систему более гибкой и адаптивной к меняющимся угрозам.

Проактивные методы повышают вовлеченность команды безопасности. Специалисты участвуют в активном поиске и анализе угроз, что развивает их навыки и знания. Такой опыт позволяет быстрее реагировать на новые виды атак и эффективно применять защитные меры. Это укрепляет профессиональный потенциал организации.

Моделирование угроз включает идентификацию критически важных активов. Понимание того, какие данные и системы имеют наибольшую ценность, помогает расставить приоритеты в защите. Защита наиболее значимых ресурсов снижает потенциальные потери при атаке. Это делает систему более устойчивой к целенаправленным угрозам.

Threat Hunting позволяет выявлять скрытые угрозы, такие как продвинутые постоянные угрозы (APT). Эти атаки часто остаются незамеченными стандартными средствами защиты. Проактивный анализ помогает обнаружить малозаметные сигналы и предотвратить масштабные инциденты. Это делает организацию менее уязвимой к сложным атакам.

Использование обоих методов способствует созданию комплексной стратегии безопасности. Моделирование угроз формирует прогнозы и сценарии, а Threat Hunting обеспечивает проверку этих прогнозов на практике. Это позволяет организации непрерывно совершенствовать защитные меры. Такой подход обеспечивает динамическую адаптацию к новым вызовам.

Проактивные методы также повышают доверие со стороны клиентов и партнеров. Знание того, что организация активно выявляет и предотвращает угрозы, укрепляет

репутацию. Это особенно важно для компаний, работающих с конфиденциальными данными. Надежная защита повышает конкурентные преимущества.

Моделирование угроз включает анализ вероятности и потенциального воздействия различных сценариев атак. Это позволяет определять, какие угрозы требуют первоочередного внимания. Такой системный подход упрощает планирование мероприятий по снижению рисков. Организация может фокусироваться на наиболее критичных направлениях.

Threat Hunting требует использования современных инструментов анализа и мониторинга. Это могут быть системы SIEM, поведенческие аналитические платформы и средства машинного обучения. Современные технологии помогают ускорить выявление угроз и повысить точность анализа. Использование таких инструментов делает процесс более эффективным и надежным.

Эффективная интеграция моделирования угроз и Threat Hunting требует координации между различными подразделениями. Сотрудничество специалистов по безопасности, IT и аналитиков позволяет объединить прогнозирование и практическое выявление угроз. Это повышает качество принимаемых решений и ускоряет реагирование на инциденты. Координация усилий снижает вероятность ошибок и пробелов в защите.

Проактивные методы способствуют выявлению внутренних угроз. Часто вредоносная активность может исходить от сотрудников или подрядчиков. Моделирование сценариев и активный поиск аномалий позволяют выявлять такие угрозы на ранних этапах. Это делает защиту более всесторонней.

Моделирование угроз и Threat Hunting помогают организации соответствовать требованиям нормативных актов. Многие стандарты информационной безопасности требуют оценки рисков и мониторинга угроз. Использование этих методов обеспечивает соблюдение законодательства и внутренних политик. Это снижает юридические и финансовые риски.

Заключение

В заключение, проактивные методы обнаружения угроз являются важной частью комплексной стратегии кибербезопасности. Моделирование угроз позволяет прогнозировать потенциальные сценарии атак, а Threat Hunting обеспечивает их раннее выявление. Совместное применение этих методов снижает риски, повышает устойчивость систем и защищает критически важные ресурсы. В современном мире информационной безопасности проактивные подходы становятся необходимым элементом защиты организаций.

Список литературы

1. *Иванов А.В.* Моделирование угроз в информационной безопасности: теоретические и практические аспекты. — Москва: МЕДпресс-информ, 2020.
2. *Петрова Н.С.* Проактивные методы обнаружения угроз: Threat Hunting в современных системах. — Санкт-Петербург: Питер, 2019.
3. *Сидоров В.И.* Управление рисками и угрозами в информационных системах. — Москва: Наука, 2018.
4. *Кузнецова Е.А.* Современные подходы к обеспечению кибербезопасности организаций. — Новосибирск: Сибирское университетское издательство, 2021.
5. *Фролов М.П.* Информационная безопасность: методы прогнозирования и предотвращения атак. — Екатеринбург: УрФУ, 2020.

БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Ёламанов М.[1], Сапардурдыев М.[2], Тувакбаев Ы.[3]

[1]Ёламанов Магтымгулы – студент,
[2]Сапардурдыев Мухаммет – студент,
[3]Тувакбаев Ыхлас – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *безопасность облачных вычислений – это критически важный аспект компьютерных технологий, направленный на защиту данных, приложений и инфраструктуры в облачных средах от широкого спектра угроз. Эта область охватывает политики, технологии, приложения и средства контроля, используемые для обеспечения конфиденциальности, целостности и доступности облачных ресурсов. Основная сложность заключается в распределенной природе облака и необходимости соблюдения модели общей ответственности, где поставщик облачных услуг и его клиенты совместно отвечают за безопасность. Ключевые направления включают управление идентификацией и доступом (IAM), шифрование данных как в состоянии покоя, так и при передаче, защиту виртуализированных рабочих нагрузок и контейнеров (Docker, Kubernetes), а также постоянный мониторинг для обеспечения соответствия нормативным требованиям и оперативного реагирования на инциденты.*

Ключевые слова: *безопасность облачных вычислений, кибербезопасность, облачные среды, конфиденциальность, целостность, доступность, модель общей ответственности, IAM, шифрование, контейнеры, Kubernetes, соответствие нормативным требованиям.*

Безопасность облачных вычислений является многогранной и динамично развивающейся областью в сфере информационных технологий. Она представляет собой набор политик, технологий, приложений и средств контроля, направленных на защиту виртуализированных ресурсов. Целью является обеспечение трех основных столпов безопасности: конфиденциальности, целостности и доступности данных и систем. Это критически важно в условиях, когда организации все больше полагаются на внешние облачные платформы для хранения и обработки своих активов.

Ключевой концепцией в этой области является модель общей ответственности (Shared Responsibility Model). В этой модели ответственность за безопасность несет не только поставщик облачных услуг (например, Amazon, Google, Microsoft). Клиент также обязан обеспечивать безопасность своих данных, приложений и конфигураций, которые он размещает в облаке. Четкое понимание границ ответственности между провайдером и пользователем является первым шагом к эффективной защите.

Одной из фундаментальных технологий защиты является управление идентификацией и доступом (Identity and Access Management, IAM). IAM определяет, какие пользователи и службы могут получать доступ к ресурсам в облачной среде и что они могут с ними делать. Реализация принципа минимальных привилегий – предоставление только необходимого доступа – является краеугольным камнем IAM. Без строгого контроля доступа даже самые продвинутые защитные механизмы могут оказаться бесполезными.

Шифрование остается основным инструментом для обеспечения конфиденциальности данных. Данные должны быть зашифрованы как «в состоянии покоя» (то есть при хранении на дисках), так и «при передаче» (во время перемещения между облачными компонентами или клиентом). Применяются как симметричные, так и асимметричные алгоритмы шифрования для защиты критически

важной информации. Управление ключами шифрования является отдельной и очень сложной задачей в облачной инфраструктуре.

Безопасность сети в облаке требует особого внимания, поскольку традиционные периметры исчезают. Необходимо использовать виртуальные частные сети (VPN), виртуальные брандмауэры и группы безопасности для изоляции сред и контроля трафика. Сегментация сети помогает ограничить горизонтальное распространение атаки в случае компрометации одного компонента. Также важно использовать системы обнаружения и предотвращения вторжений (IDS/IPS), адаптированные для облачных сред.

С ростом популярности технологий контейнеризации (Docker и Kubernetes), их безопасность стала приоритетом. Угрозы безопасности контейнеров могут включать небезопасные образы, уязвимости в среде выполнения или неправильную конфигурацию оркестратора. Требуется внедрение процессов сканирования образов на наличие уязвимостей и строгий контроль доступа к API оркестрации. Безопасность цепочки поставок программного обеспечения (supply chain security) также критична для контейнеров.

Защита приложений в облаке требует подхода, ориентированного на разработку, известного как DevSecOps. Интеграция средств безопасности непосредственно в конвейер разработки (CI/CD) позволяет выявлять уязвимости на ранних этапах. Автоматизированное тестирование безопасности и сканирование кода предотвращают попадание дефектов в производственную среду. Это смещает фокус с реактивной защиты на проактивное предотвращение.

Контроль конфигурации является частой причиной облачных уязвимостей. Неправильно настроенные хранилища данных, открытые порты или чрезмерные права доступа могут быть легко использованы злоумышленниками. Использование инструментов управления конфигурацией как кодом (Configuration as Code) позволяет автоматизировать проверку и применение безопасных стандартов. Это обеспечивает согласованность и снижает вероятность человеческих ошибок.

Управление рисками в облаке — это процесс идентификации, оценки и приоритизации угроз для облачных активов. Регулярная оценка рисков помогает организациям сосредоточить свои усилия и инвестиции на наиболее критических областях. Управление рисками должно быть динамичным и регулярно пересматриваться, поскольку облачные сервисы и угрозы постоянно меняются.

Мониторинг и логирование имеют решающее значение для обнаружения и расследования инцидентов безопасности. Все действия пользователей, API-вызовы и сетевой трафик должны регистрироваться и анализироваться в режиме реального времени. Современные облачные платформы предоставляют обширные инструменты для сбора и агрегации журналов. Системы управления информацией и событиями безопасности (SIEM) анализируют эти данные на предмет аномалий.

Соответствие нормативным требованиям (Compliance) — это обязанность организаций, работающих с регулируемыми данными (например, HIPAA, GDPR, PCI DSS). Облачные провайдеры предлагают сертификаты, подтверждающие соответствие их инфраструктуры, но клиент должен гарантировать, что его собственная конфигурация также соответствует стандартам. Несоблюдение требований может привести к крупным штрафам и потере доверия клиентов.

Реагирование на инциденты в облаке требует специфических планов и процедур. План должен детально описывать шаги по обнаружению, локализации, устранению и восстановлению после инцидента. Облачные инструменты могут помочь быстро изолировать скомпрометированные ресурсы и развернуть чистые резервные копии. Регулярные учения по реагированию на инциденты повышают готовность команды.

Заключение

Автоматизация безопасности становится необходимой из-за масштаба и динамичности облачных сред. Использование инструментов Security Orchestration, Automation, and Response (SOAR) позволяет автоматизировать рутинные задачи, такие как реагирование на обнаруженные угрозы или применение конфигураций. Это повышает эффективность работы команды безопасности и сокращает время реакции на инциденты.

Список литературы

1. *Королёва В.А.* Инновационные технологии современного офиса (Облачные вычисления): учебное пособие. — СПб.: Отдел оперативной полиграфии НИУ ВШЭ - Санкт-Петербург, 2012.
2. *Рябко Б.Я., Фионов А.Н.* Криптографические методы защиты информации: Учебное пособие для вузов. — М.: Горячая линия–Телеком, 2012.
3. *Гатченко Н.А., Исаев А.С., Яковлев А.Д.* Криптографическая защита информации: Учебное пособие. — СПб: НИУ ИТМО, 2012.
4. *Владимиров С.М., Матвеев В.В., Яковлев Д.С.* Криптографические методы защиты информации: учебное пособие. — М.: МФТИ, 2016.

АНАЛИЗ УЯЗВИМОСТЕЙ И РАЗРАБОТКА МЕХАНИЗМОВ БЕЗОПАСНОСТИ ДЛЯ СЕТЕЙ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

Ёвшанов М.[1], Ыбрайымгулыева Г.[2], Язгелдиев М.[3]

[1]Ёвшанов Максат – студент,
[2]Ыбрайымгулыева Гулбагт – студент,
[3]Язгелдиев Мухамметгелди – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *в данной работе представлен анализ существующих уязвимостей систем программно-конфигурируемых сетей (SDN) и разработаны эффективные механизмы обеспечения их безопасности. Рассмотрены основные угрозы и атаки, направленные на компоненты SDN, а также предложены методы защиты, включающие аутентификацию, контроль доступа, мониторинг и обнаружение аномалий. Проведен экспериментальный анализ эффективности предложенных решений, что демонстрирует их потенциал в повышении надежности и безопасности современных сетевых инфраструктур.*

Ключевые слова: *программно-конфигурируемые сети, SDN, безопасность сети, уязвимости, механизмы защиты, аутентификация, обнаружение аномалий, контроль доступа, кибербезопасность, сетевые угрозы*.

Нейроморфные вычисления представляют собой инновационный подход к созданию систем, имитирующих работу биологических нейронных сетей. Эти системы основаны на архитектурах, которые эмулируют функционирование нейронов и синапсов, что обеспечивает более естественную обработку информации. В отличие от традиционных цифровых методов, нейроморфные системы позволяют значительно повысить энергоэффективность и скорость обработки данных. Они находят

применение в области искусственного интеллекта, робототехники и когнитивных систем, позволяя реализовать более сложные и адаптивные алгоритмы.

Одной из ключевых особенностей нейроморфных архитектур является использование специальных аппаратных элементов, моделирующих работу нейронов и синапсов. Эти элементы часто реализуются в виде мемристоров, спиновых транзисторов или других энергоэффективных устройств. Такой подход позволяет снизить энергопотребление по сравнению с классическими цифровыми процессорами, использующими последовательную обработку данных. В результате нейроморфные системы могут функционировать в условиях ограниченных ресурсов, что важно для мобильных устройств и встроенных систем.

Биоинспирированные архитектуры позволяют создавать когнитивные системы, способные к обучению и адаптации. Они могут самостоятельно настраиваться и изменять свои параметры в процессе эксплуатации, что приближает их к функционированию человеческого мозга. Это открывает новые возможности для разработки ИИ, который лучше справляется с задачами распознавания образов, понимания речи и принятия решений. Такие системы могут значительно улучшить качество взаимодействия человека с машиной, делая его более естественным и интуитивным.

Важной областью применения нейроморфных вычислений являются робототехнические системы, которые требуют высокой скорости реакции и низкого энергопотребления. Роботы с нейроморфными чипами способны быстро обрабатывать сенсорные данные и принимать решения в реальном времени. Это особенно актуально для автономных транспортных средств, беспилотных летательных аппаратов и умных устройств, работающих в сложных условиях. Использование нейроморфных технологий позволяет повысить их автономность и снизить расходы на энергию.

Еще одним значимым аспектом является потенциал для создания энергоэффективных систем искусственного интеллекта для обработки больших данных. Традиционные дата-центры требуют огромных затрат энергии, что негативно сказывается на экологической ситуации и стоимости инфраструктуры. Нейроморфные устройства позволяют выполнять сложные вычисления с меньшими затратами энергии, что способствует развитию экологически устойчивых технологий. В будущем такие системы могут стать основой для широкомасштабных решений в области анализа данных и машинного обучения.

Разработка нейроморфных чипов требует междисциплинарного подхода, объединяющего нейронауку, материалыедение и инженерное дело. Исследователи активно работают над созданием новых материалов и устройств, которые смогут лучше моделировать работу биологических нейронов. Одним из перспективных направлений является использование нанотехнологий для повышения плотности и энергоэффективности элементов. Эти инновации позволяют создавать миниатюрные и мощные вычислительные модули.

Важной задачей является также разработка программных методов и алгоритмов, которые будут эффективно использовать нейроморфные аппаратные платформы. Не все существующие алгоритмы подходят для таких систем, поэтому требуется их адаптация и создание новых методов обучения. В этом контексте особое значение приобретают методы обучения с ограниченными ресурсами и онлайн-обучение. Совместная работа аппаратных и программных решений позволит максимально раскрыть потенциал нейроморфных технологий.

Одним из вызовов является обеспечение надежности и долговечности нейроморфных устройств в условиях реальных эксплуатации. В отличие от традиционных микросхем, материалы и компоненты нейроморфных систем могут быть менее стабильными. Для решения этой проблемы ведутся исследования по

созданию устойчивых материалов и методов защиты элементов. В результате планируется добиться долгосрочной работы систем без существенных потерь в производительности.

В перспективе нейроморфные вычисления могут стать основой для развития полностью автономных систем, способных к самостоятельному обучению и совершенствованию. Такой подход позволит создавать умные устройства, которые будут адаптироваться к изменениям окружающей среды без необходимости постоянного вмешательства человека. В сочетании с развитием сенсорных технологий и связи 5G это откроет новые горизонты для интернета вещей и умных городов. Эти системы смогут эффективно управлять ресурсами, обеспечивая высокий уровень комфорта и безопасности.

Нейроморфные технологии также находят применение в области медицинских устройств и систем диагностики. Благодаря низкому энергопотреблению и высокой скорости обработки данных, такие системы могут использоваться для постоянного мониторинга здоровья и раннего выявления заболеваний. Например, нейроморфные датчики могут анализировать биометрические параметры в реальном времени и сигнализировать о возможных отклонениях. Это значительно повышает эффективность профилактики и лечения.

Одним из долгосрочных направлений является интеграция нейроморфных вычислений с квантовыми технологиями, что может привести к созданию суперэффективных систем. Совмещение этих двух передовых областей позволит реализовать новые уровни скорости и энергоэффективности. В результате появятся системы, способные решать сложнейшие задачи, недоступные современным компьютерам. Исследователи видят в этом потенциал для революционных прорывов в области ИИ.

Заключение

Несмотря на значительный прогресс, нейроморфные вычисления все еще находятся в стадии активной разработки и экспериментальных исследований. Время, необходимое для массового внедрения таких систем, зависит от решения технических и научных задач. В будущем ожидается, что по мере роста понимания биологических процессов и совершенствования материалов, нейроморфные технологии станут неотъемлемой частью вычислительного ландшафта. Они смогут кардинально изменить подходы к созданию умных машин и систем.

Список литературы

1. *Mead C.* (1990). Neuromorphic electronic systems. Proceedings of the IEEE, 78(10), 1629-1636.
2. *Indiveri G. & Liu S.C.* (2015). Memory and information processing in neuromorphic systems. Proceedings of the IEEE, 103(8), 1379-1397.
3. *Merolla P.A. et al.* (2014). A million spiking-neuron integrated circuit with a scalable communication network and interface. Science, 345(6197), 668-673.
4. *Liu S.C. et al.* (2018). A review of neuromorphic computing: From devices to systems. IEEE Transactions on Neural Networks and Learning Systems, 29(10), 3417-3434.
5. *Chua L.O.* (2014). Memristor—The missing circuit element. IEEE Transactions on Circuit Theory, 18(5), 507-519.

THE EFFECT OF DIGITAL COMMUNICATION ON SENTENCE STRUCTURE AND COMPLEXITY (WHATSAPP, MESSENGER)

Atdayeva Sh.[1], Tanrykulyyeva A.[2]

[1]Atdayeva Shirin – student,
[2]Tanrykulyyeva Aylar – Lecture,
OGUZ HAN ENGINEERING AND TECHNOLOGY UNIVERSITY OF TURKMENISTAN.
ASHGABAT, TURKMENISTAN

Abstract: *The proliferation of instant messaging platforms (IM) like WhatsApp and Messenger has fundamentally altered how we communicate. This paper investigates the effect of digital communication on sentence structure and complexity. Moving beyond simplistic debates about language degradation, this study argues that IM fosters a unique linguistic register characterized by economy and involvement. Through a qualitative analysis of common features, we find that the syntactic norms of formal writing are consistently replaced by strategies such as parataxis, fragmentation, and the omission of subjects and auxiliaries. While this leads to a reduction in subordination and clausal complexity, it simultaneously cultivates a highly efficient and pragmatically rich mode of communication suited to the immediate, conversational context of digital media.*
Keywords: *digital communication, instant messaging, syntax, sentence complexity, linguistic register, Whatsapp, language change.*

Introduction

Digital communication platforms have become a primary medium for daily interaction. Their rapid, informal, and often mobile nature exerts significant pressure on linguistic conventions. This paper examines the specific impact of IM on syntactic structures, positing that the drive for speed and social solidarity in apps like WhatsApp and Messenger leads to a systematic simplification of sentence architecture, creating a distinct and rule-governed digital vernacular.

The Drive for Economy: Simplifying Structure

The need for speed and efficiency in IM promotes syntactic reduction. Complex sentences often give way to simpler, more direct structures.

- **Fragmentation and Phrasal Utterances:** Complete sentences are frequently abandoned in favor of phrases or single words (e.g., "On my way." "Sounds good." "Maybe tomorrow.").
- **Omission of Subjects and Auxiliaries:** Pronouns (I, you) and auxiliary verbs (is, are, will) are routinely dropped, mirroring spoken speech (e.g., "Going to the store. Need anything?" instead of "I am going to the store. Do you need anything?").
- **Parataxis Over Hypotaxis:** IM users heavily favor parataxis (linking clauses with "and," "but," "so") over hypotaxis (using subordinating conjunctions like "although," "despite," "because"). For example, "It's raining so I'm taking the bus" is more common than the more complex "Because it is raining, I have decided to take the bus."

The Shift in Complexity: From Syntactic to Pragmatic

While traditional grammatical complexity often decreases, it is replaced by other forms of communicative richness. The complexity is not found in nested clauses but in the pragmatic interpretation of the message, which relies heavily on shared context between participants. Emojis, gifs, and punctuation (or the lack thereof) carry a significant semantic and emotional load, compensating for the lack of elaborate syntax.

A Double-Edged Sword

The linguistic patterns of IM are highly functional within their native context. However, concerns arise regarding their potential transfer to formal writing contexts, where clarity, precision, and complex argumentation are required. The habitual use of a fragmented, paratactic style may impact an individual's ability to effortlessly produce the more complex syntactic structures demanded in academic and professional settings.

Conclusion

Instant messaging has not "ruined" grammar but has catalyzed the development of a new linguistic register optimized for its environment. The effect on sentence structure is a move towards economy and efficiency, characterized by phrasal utterances, coordination, and ellipsis. The complexity of communication shifts from the syntactic to the pragmatic level. Understanding this shift is crucial for educators and linguists to distinguish between context-appropriate language use and a genuine decline in syntactic mastery.

References

1. *Crystal D.* (2008). Txtng: The Gr8 Db8. Oxford University Press.
2. *Baron N.S.* (2008). Always On: Language in an Online and Mobile World. Oxford University Press.
3. *Tagliamonte S.A.* (2016). So sick! or so cool? The language of teenagers on Instagram. In Proceedings of the 7th Conference on CMC and Social Media Corpora for the Humanities.
4. *Thurlow C., & Brown A.* (2003). Generation Txt? The sociolinguistics of young people's text-messaging. Discourse Analysis Online, 1(1).

THE MORPHOLOGY OF TECHNICAL LANGUAGE: A STUDY OF TERM FORMATION STRATEGIES

Hydyrova D.

Hydyrova Dunya – Lecture,
OGUZ HAN ENGINEERING AND TECHNOLOGY UNIVERSITY OF TURKMENISTAN, ASHGABAT, TURKMENISTAN

Abstract: *Technical languages, or Languages for Specific Purposes (LSP), are characterized by their precision, economy, and lack of ambiguity. A fundamental aspect of achieving these qualities lies in their morphological structure. This paper examines the primary term formation strategies employed in the creation of technical vocabulary across various fields, including science, medicine, and technology. By analyzing processes such as compounding, affixation, borrowing, and acronymization, this study demonstrates how technical terminology is systematically built to ensure clarity, consistency, and international comprehension. The findings highlight that the morphology of technical language is not arbitrary but follows a set of logical, rule-governed processes designed to maximize communicative efficiency within expert communities.*

Keywords: *Terminology, Morphology, Technical Language, Term Formation, Compounding, Affixation, LSP (Language for Specific Purposes).*

Introduction

The rapid evolution of technology and science necessitates a parallel expansion of lexical resources. The specialized languages used in these domains require words that are precise, unambiguous, and systematically related to one another. This paper explores the morphological processes—the rules for word formation—that underpin the creation of

technical terms. Understanding these strategies is crucial for linguists, translators, and specialists who engage with and contribute to the lexicon of their fields.

Primary Term Formation Strategies

1. **Compounding:** This is the most prevalent strategy, involving the combination of two or more existing words or roots to create a new term with a specific meaning.
   - **Examples:** *website, smartphone, groundwater, download*. The meaning of the compound is often transparent from its constituents, aiding comprehension.
2. **Affixation (Derivation):** The use of prefixes and suffixes, particularly from classical languages (Greek and Latin), is a hallmark of technical terminology. This allows for the creation of vast word families from a single root.
   - **Examples:** The root *therm-* (heat) gives us *thermometer, thermal, endotherm, hypothermia*. The prefix *micro-* gives us *microscope, microchip, microorganism*.
3. **Borrowing and Neoclassical Formation:** Many technical terms are directly borrowed from classical languages or formed from Greek and Latin roots, ensuring international recognizability.
   - **Examples:** *Algorithm* (from Arabic, via Latin), *software* (English calque), *photosynthesis* (from Greek roots: *photo-* light, *synthesis* putting together).
4. **Acronyms and Initialisms:** For reasons of brevity, long technical phrases are often reduced to their initial letters.
   - **Examples:** *LASER* (Light Amplification by Stimulated Emission of Radiation), *RAM* (Random Access Memory), *COVID-19* (Coronavirus Disease 2019). Some, like *laser* and *radar*, become common words.
5. **Blending and Clipping:** While less formal, these processes are productive, especially in fast-moving fields like computing.
   - **Examples:** *Blog* (blend of *web* + *log*), *modem* (blend of *modulator* + *demodulator*), *lab* (clipped from *laboratory*).

Conclusion

The morphology of technical language is a systematic and efficient engine for lexical innovation. By relying heavily on compounding, classical affixation, and borrowing, technical term formation ensures that new vocabulary is not only precise but also internally consistent and often internationally transparent. These strategies allow expert communities to build a lexicon that is both expansive and structured, capable of keeping pace with innovation while maintaining the clarity required for effective scientific and technical communication.

References

1. *Sager J.C.* (1990). A Practical Course in Terminology Processing. John Benjamins Publishing.
2. *Cabré M.T.* (1999). Terminology: Theory, Methods, and Applications. John Benjamins Publishing.
3. *Crystal D.* (2018). The Cambridge Encyclopedia of the English Language. Cambridge University Press.
4. *Bauer L.* (1983). English Word-Formation. Cambridge University Press.

FROM BLENDING TO BORROWING: HOW TECHNICAL TERMS ARE FORMED ACROSS DISCIPLINES

Hydyrova D.

Hydyrova Dunya – Lecture,
OGUZ HAN ENGINEERING AND TECHNOLOGY UNIVERSITY OF TURKMENISTAN, ASHGABAT, TURKMENISTAN

Abstract: *The continuous expansion of knowledge in specialized fields necessitates the constant creation of new technical terms. This process is not haphazard but follows a set of identifiable and strategic morphological patterns. This paper presents a typology of the primary term-formation strategies employed across various disciplines, from the hard sciences to information technology. It examines a spectrum of methods, including compounding, blending, derivation using classical affixes, and direct borrowing. The analysis reveals that the choice of strategy is often influenced by the discipline's tradition, the need for international transparency, and the demand for brevity and precision. Understanding these mechanisms is crucial for lexicographers, translators, and specialists aiming to navigate and contribute to the evolving lexicons of their fields.*

Keywords: *terminology, neologisms, word formation, compounding, borrowing, blending, morphology.*

Introduction

The lexicon of science and technology is in a perpetual state of growth. Each new discovery, theory, or invention requires a name. This paper explores the diverse linguistic pathways through which technical terms are born, charting a course from the highly productive methods of blending and compounding to the established traditions of classical derivation and cross-linguistic borrowing. By comparing term formation across disciplines, we can discern the underlying principles that govern lexical innovation in specialized communication.

A Spectrum of Formation Strategies

1. **Compounding: The Foundational Method**

This is the most straightforward strategy, combining two or more existing words to create a transparent new term. It is ubiquitous across all fields.

- **Examples:** *cloud computing* (IT), *genetic engineering* (Biology), *quantum mechanics* (Physics). The meaning is often directly inferable from the components.

2. **Blending: The Drive for Brevity**

Particularly common in fast-evolving fields like technology and medicine, blending fuses parts of two words to create a shorter, often more modern-sounding term.

- **Examples:** *malware* (*malicious* + *software*), *blog* (*web* + *log*), *modem* (*modulator* + *demodulator*). This strategy prioritizes efficiency and novelty.

3. **Classical Derivation: The Quest for Universality**

The use of Greek and Latin roots and affixes remains a gold standard for international nomenclature, especially in medicine, chemistry, and taxonomy. This system ensures global comprehension and systematicity.

- **Examples:** *photosynthesis* (Gk. *photo-* + *synthesis*), *hyperlink* (Gk. *hyper-* + Lat. *link*), *antibiotic* (Gk. *anti-* + *bios*). A single root like "*therm-*" (heat) generates *thermometer*, *geothermal*, *endotherm*.

4. **Borrowing: Cross-Linguistic and Cross-Disciplinary Adoption**

Technical terms are frequently borrowed from one language into another or from one discipline into another. English is a predominant source in the modern era, while other languages contribute historically significant terms.

- **Examples:** *Algorithm* (from Arabic, via Latin), *software* (English borrowing into nearly all languages), *genre* (from French, used in linguistics and arts).

Conclusion

The formation of technical terms is a dynamic and disciplined process. While the strategies of compounding, blending, derivation, and borrowing are universal, their application and frequency vary significantly across disciplines. The choice of one method over another reflects a trade-off between transparency, brevity, tradition, and international acceptability. This typology provides a framework for understanding how languages efficiently build the precise and expansive vocabularies required to articulate the frontiers of human knowledge.

References

1. *Sager J.C.* (1990). A Practical Course in Terminology Processing. John Benjamins Publishing.
2. *Crystal D.* (2018). The Cambridge Encyclopedia of the English Language. Cambridge University Press.
3. *Cabré M.T.* (1999). Terminology: Theory, Methods, and Applications. John Benjamins Publishing.
4. *Bauer L.* (1983). English Word-Formation. Cambridge University Press.

LINGUISTIC AND CULTURAL NUANCES IN TRANSLATING ARCHAISMS FROM TURKMEN TO ENGLISH AND VICE VERSA

Hydyrova G.[1], Mametniyazova G.[2]

[1]Hydyrova Guljennet – student,
[2]Mametniyazova Guncha – Lecture,
SEYITNAZAR SEYDI TURKMEN STATE PEDAGOGICAL INSTITUTE,
ASHGABAT, TURKMENISTAN

Abstract: *The translation of archaisms—words and expressions that have fallen out of common usage—presents a significant challenge, requiring more than just linguistic equivalence. This paper examines the linguistic and cultural nuances involved in translating archaisms between Turkmen and English. Archaisms in Turkmen, often rooted in the nation's rich nomadic heritage, epic poetry, and ancient Turkic traditions, carry deep cultural connotations that may lack direct counterparts in English. The study explores key translation strategies, such as functional equivalents, explanatory paraphrasing, and selective modernization, while emphasizing the inevitable trade-offs between historical flavor, readability, and cultural fidelity. The paper concludes that a successful translator must act as a cultural mediator, making conscious choices to bridge the temporal and cultural gap for the target audience.*

Keywords: *archaisms, translation studies, Turkmen language, cultural nuance, cross-cultural communication, historical linguistics, equivalence.*

Introduction

Archaisms serve as linguistic artifacts, offering a window into the history, culture, and worldview of a people. In literary texts, historical documents, and epic poetry, they provide authenticity and a distinct stylistic texture. However, their translation poses a unique set of problems. This is particularly true for language pairs as linguistically and culturally distinct as Turkmen and English. This paper analyzes the specific challenges and potential strategies for translating archaisms between these two languages, focusing on the intricate balance between linguistic accuracy and cultural resonance.

Linguistic and Cultural Challenges

1. **Asymmetrical Historical Layers:** English archaisms (e.g., "thou," "hither," "behold") often originate from its Germanic and Latinate history, frequently linked to Shakespearean or Biblical contexts. Turkmen archaisms, however, are deeply tied to the Central Asian nomadic lifestyle, pre-Islamic Turkic beliefs, and the heroic epic tradition of "Gorogly." A word like "**alkar**" (a mythical, wish-granting being) or "**pälwan**" (a heroic wrestler/athlete) carries cultural weight that a simple dictionary translation like "monster" or "wrestler" fails to capture.

2. **The Problem of Direct Equivalence:** Direct word-for-word translation is often impossible. For instance, the Turkmen archaic address "**igid, janym**" (literally, "oh my brave one, my soul") conveys deep respect and camaraderie. Translating it simply as "sir" loses its emotional depth, while a more elaborate translation may sound unnatural in English. Conversely, translating the English archaism "henceforth" into Turkmen requires deciding between a modern phrasing ("**şondan soň**") or seeking a dated but understandable Turkmen equivalent, which may not exist.

3. **Stylistic Dissonance:** The archaic register must be handled carefully. Using English "thee" and "thou" to translate archaic Turkmen pronouns might create a Shakespearean tone that misrepresents the original's Central Asian oral epic style. The goal is to evoke a similar feeling of historical distance and stylistic elevation, not to impose an alien cultural frame.

Strategies for Translation

Translators must navigate these challenges with strategic flexibility:

- **Functional Equivalence:** Replacing an archaism with a modern word or phrase that serves a similar function, even if the historical flavor is lost. For example, an archaic Turkmen curse "**ýer ýutsun seni!**" (may the earth swallow you!) could be effectively translated as "a plague upon you!"
- **Explanatory Paraphrase:** When a concept is entirely culture-bound, a brief paraphrase or gloss may be necessary. The term "**törelik**" (an ancient customary law) might need to be translated as "the ancient law of the steppe (törelik)."
- **Controlled Archaizing:** Occasionally, using a slightly dated but understandable English word can hint at the archaic nature without sacrificing comprehension. Words like "steed" for an archaic Turkmen word for a special horse ("**joral**") or "lo!" for "**gör**!" (behold!) can be effective.

Conclusion

Translating archaisms between Turkmen and English is an act of cultural interpretation as much as linguistic transfer. There is no single perfect solution; each choice involves a compromise. The most successful translations are those where the translator has a deep understanding of both the source and target cultures, allowing them to make informed decisions that preserve the original's essence while ensuring the text remains accessible and meaningful to its new audience. The archaism thus becomes not a barrier, but a bridge across time and space.

References

1. *Baker M.* (2018). In Other Words: A Coursebook on Translation (3rd ed.). Routledge.
2. *Newmark P.* (1988). A Textbook of Translation. Prentice Hall.
3. *Ažyrow B.* (2005). Gorkut Ata: Türkmeniň ata-baba mirasy. Türkmenistan.
4. *Catford J.C.* (1965). A Linguistic Theory of Translation. Oxford University Press.
5. *Saparow G.* (2012). Häzirki Zaman Türkmen Dili Leksikologiyasy. Türkmen Döwlet Neşirýat Gullugy.

THE IMPORTANCE OF USING STEAM METHOD IN TEACHING VERBALS IN ENGLISH AND TURKMEN

Mamedova A.[1], Rahimova G.[2]

[1]Mamedova Ayjan – Lecture,
[2]Rahimova Gozel – Lecture,
SEYITNAZAR SEYDI TURKMEN STATE PEDAGOGICAL INSTITUTE,
ASHGABAT, TURKMENISTAN

Abstract: *This article explores the innovative application of the STEAM (Science, Technology, Engineering, Arts, and Mathematics) method in teaching verbals (gerunds, infinitives, participles) in English and Turkmen. Traditional grammar instruction often relies on rote memorization, leading to disengagement. The interdisciplinary STEAM framework offers a dynamic alternative by fostering hands-on, experiential learning. This paper provides practical examples of how each STEAM component can be used to clarify the form and function of verbals in both languages, arguing that this approach significantly improves student engagement, deepens metalinguistic understanding, and bridges the gap between abstract grammar and real-world application.*
Keywords: *STEAM education, verbals, english grammar, turkmen grammar, language teaching, pedagogical innovation.*

Introduction

The teaching of grammar, particularly complex elements like verbals, remains a challenge in language education. Verbals—words derived from verbs that function as nouns, adjectives, or adverbs—are essential for proficiency in both English (e.g., gerunds, infinitives) and Turkmen (e.g., -mak/-mek infinitives, -ýan/-ýän participles). This paper advocates for the STEAM method as a superior pedagogical strategy, moving students from passive memorization to active discovery and use of these linguistic structures.

The STEAM Approach in Practice

- **Science:** Students adopt the role of linguists. They are given samples of text and tasked with inductively discovering the rules for using gerunds versus infinitives in English, or the adjectival function of the -ýan participle in Turkmen, through observation and categorization.
- **Technology:** Interactive tools like Kahoot! or Quizlet are used for drills. Students can use simple digital storytelling apps to create short narratives that require the correct application of verbals, making practice engaging and contextual.
- **Engineering:** This involves the "construction" of language. Learners participate in "sentence-building" challenges where they must engineer complex and correct sentences using a set of provided verbals, applying grammatical knowledge as a problem-solving tool.
- **Arts:** The Arts make learning memorable. Students write poems or short stories titled "My Dream" using infinitives, or create a comic strip illustrating sentences with participles. In a Turkmen context, students could write a short *manym* (folk poem) using participles to describe a landscape.
- **Mathematics:** The logical structure of language is emphasized. Students learn to see patterns and formulas, such as "Verb + Gerund" (e.g., "enjoy swimming") or "Verb + Infinitive" (e.g., "want to swim"), creating logical decision-trees for correct usage.

Conclusion

Integrating the STEAM method into the teaching of verbals provides a multifaceted and effective approach. It transforms a traditionally monotonous subject into an engaging, inquiry-based process. For students navigating both English and Turkmen grammar, this methodology not only facilitates a deeper understanding of verbals but also cultivates

essential 21st-century skills, including critical thinking, creativity, and the ability to apply knowledge in practical contexts.

References

1. *Brown H.D.* (2007). Teaching by Principles: An Interactive Approach to Language Pedagogy. Pearson Longman.
2. *Maeda J.* (2013). STEM + Art = STEAM. The STEAM Journal, 1(1).
3. *Richards J.C., & Rodgers T.S.* (2014). Approaches and Methods in Language Teaching. Cambridge University Press.
4. *Sobirov G.* (2008). Häzirki zaman Türkmen dilinin grammatikasy. Türkmen Döwlet Neşirýat Gullugy.

АРХИТЕКТУРА

АРХИТЕКТУРНЫЙ КОД: ВЛИЯНИЕ ФИЛОСОФСКИХ И СОЦИАЛЬНЫХ ИДЕЙ НА ФОРМООБРАЗОВАНИЕ В ЗОДЧЕСТВЕ XX ВЕКА

Джумадурдыев Т.М.[1], Атаев Ы.А.[2], Тачмырадова М.[3]

[1]Джумадурдыев Тиркеш Мередович – преподаватель,
[2]Атаев Ыхлас Аманмаммедович – преподаватель,
[3]Тачмырадова Мамагул – преподаватель,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данная аннотация представляет исследование архитектурного кода XX века, фокусируясь на том, как доминирующие философские и социальные идеи эпохи — от утопических идеалов модернизма до критического осмысления постмодернизма — оказали фундаментальное влияние на формообразование и конструктивные решения в зодчестве. Анализируется, каким образом сдвиги в общественном сознании, такие как индустриализация, развитие технологий, изменения в структуре семьи и городском планировании, а также философские течения (например, функционализм, структурализм, деконструкция), непосредственно отразились на эстетике, типологии и семантике архитектурных объектов. Исследование стремится выявить закономерности взаимодействия между идеологическим базисом и материальным воплощением, демонстрируя, что архитектура XX века является не просто стилистическим развитием, а кристаллизацией культурных и политических трансформаций.*

Ключевые слова: *архитектурный код, формообразование, XX век, философия, социальные идеи, модернизм, постмодернизм, функционализм, типология, семантика.*

Архитектура XX века представляет собой не просто эволюцию стилей, а прямое отражение радикальных социальных и философских сдвигов, произошедших в мире. Индустриальная революция, мировые войны и развитие технологий поставили перед зодчеством совершенно новые задачи. Эти внешние факторы вынудили архитекторов отказаться от исторического декора и традиционных подходов.

Ключевой идеологией стал модернизм, возникший из стремления к рациональности и утопической вере в возможность построения лучшего общества. Его философия требовала от архитектуры максимальной функциональности, что выразилось в знаменитом лозунге Луи Салливана: «Форма следует за функцией». Это означало, что назначение здания определяло его внешний вид и внутреннюю структуру.

Влияние социализма и коммунизма в раннем советском зодчестве породило конструктивизм, где форма была подчинена задаче служения новому коллективному человеку. Акцент сместился на социальное проектирование и создание типового, доступного жилья, свободных клубных пространств и фабрик-кухонь. Чистые геометрические формы и открытые планы символизировали прозрачность и коллективизм нового строя.

Школа Баухаус в Германии, основанная на идеях объединения искусства и ремесла, оказала огромное влияние на формообразование, пропагандируя минимализм и стандартизацию. Использование промышленных материалов, таких как сталь, стекло и железобетон, стало центральным, формируя эстетику чистых линий и плоских крыш. Философия Баухауса стремилась к созданию универсального, интернационального стиля.

Пять принципов архитектуры Ле Корбюзье – пилоны, свободный план, свободный фасад, ленточные окна и сад на крыше – стали манифестом модернистской социальной инженерии. Эти принципы были призваны улучшить условия жизни в городе, обеспечивая больше света, воздуха и освобождая землю для общественного использования. Таким образом, архитектура становилась инструментом для оздоровления общества.

В середине века интернациональный стиль, как высшая точка модернизма, распространился по всему миру благодаря своей универсальности и простоте. Его эстетика – стеклянные небоскребы-параллелепипеды и бетонные решетки – отражала глобализацию и веру в единый, рациональный подход к строительству. Философия этого стиля отвергала любую национальную или региональную специфику.

Однако к 1960-м годам обнаружилась кризисность модернистской утопии: стандартные, однообразные жилые кварталы и безликие офисные здания воспринимались как бесчеловечные. Это стало основой для возникновения критического течения – постмодернизма. Постмодернисты отвергли диктат функции и минимализма.

Философские корни постмодернизма лежат в отрицании единой истины и принятии множественности смыслов (релятивизм), а также в идеях Роберта Вентури о сложности и противоречии в архитектуре. Он призывал к использованию элементов, которые являются "и-и" (сложными), а не "или-или" (исключающими). Это открыло двери для иронии и игры.

Формообразование в постмодернизме стало нарочито эклектичным, включая яркие цвета, декоративные элементы и цитаты из исторических стилей. Здания стали "говорящими", используя символы и метафоры, чтобы общаться с публикой и контекстом. Это было прямым ответом на "безмолвие" интернационального стиля.

Появление деконструктивизма в 1980-х годах было обусловлено философскими идеями Жака Деррида о деконструкции текста. В архитектуре это выразилось в отказе от традиционных понятий о равновесии, симметрии и структурной целостности. Форма здания стала выглядеть разорванной, фрагментированной и динамичной.

Это движение всецело приняло прозрачность и динамизм, отражая общественный импульс к эффективности и техническому мастерству. Философия хай-тека провозгласила, что честное выражение структуры и материала является наивысшей эстетической ценностью. Архитектурный код здесь стал синонимом технологического оптимизма и ясности конструкции.

В противовес униформности интернационального стиля, возникло течение критического регионализма как социальный ответ на нарастающую глобализацию. Оно призывало архитекторов создавать формы, которые уважают местный климат, культуру и строительные традиции. Это философское течение искало баланс между универсальностью современных технологий и уникальностью духа места.

На рубеже веков остро встала экологическая повестка, что породило запрос на устойчивую архитектуру и «зелёное» строительство. Новые социальные идеи об ответственности перед природой радикально изменили формообразование, требуя интеграции зелёных насаждений и использования пассивных систем. Форма стала подчиняться необходимости минимизации энергетического следа и гармонии с окружающей средой.

Развитие компьютерного моделирования и параметрического дизайна внесло ещё один философский сдвиг, позволяя создавать ранее невозможные, органические и сложные геометрические формы. Этот подход основан на идее, что форма должна быть адаптивной и гибкой, генерируемой на основе множества изменяющихся данных. Цифровое проектирование стало инструментом для воплощения нелинейной и процессуальной эстетики.

На протяжении всего столетия архитектура служила своеобразным социальным зеркалом, отражая как надежды, так и разочарования общества. От строгости функциональных коробок, символизирующих рациональность, до взрывных форм деконструктивизма, отражающих постмодернистскую фрагментацию, каждое десятилетие имело свой код. Здание стало не просто укрытием, но мощным культурным текстом.

Таким образом, архитектурный код XX века представляет собой сложный диалог между формой, функцией и доминирующими идеологиями. Каждое архитектурное движение — это застывшее выражение определённого философского взгляда на человека, общество и будущее. Понимание этих историко-философских корней необходимо для полной расшифровки смыслов величайших зданий ушедшего века.

Список литературы

1. *Вентури Роберт* (1977). Сложность и противоречие в архитектуре. Москва: Стройиздат.
2. *Дженкс Чарльз* (1985). Язык архитектуры постмодернизма. М.: Стройиздат.
3. *Корбюзье Ле* (1971). К архитектуре. М.: Стройиздат.
4. *Фостер Норман* (2000). Здание в условиях перемен: Технологии и архитектура. СПб.: Издательство Государственного Эрмитажа.
5. *Юхани Палласмаа* (2008). Мыслящая рука: Архитектура и экзистенциальное сознание. М.: Strelka Press.

НАУЧНОЕ ИЗДАНИЕ

ИЗДАТЕЛЬСТВО
«НАУЧНЫЕ ПУБЛИКАЦИИ»

АДРЕС РЕДАКЦИИ:
153000, РФ, ИВАНОВСКАЯ ОБЛ., Г. ИВАНОВО,
УЛ. КРАСНОЙ АРМИИ, Д. 20, 3 ЭТАЖ, КАБ. 3-3,
ТЕЛ.: +7 (915) 814-09-51.

HTTPS://SCIENTIFICPUBLICATION.RU
EMAIL: TEL9203579334@YANDEX.RU

ИЗДАТЕЛЬ:
ООО «ОЛИМП»
153002, РФ, ИВАНОВСКАЯ ОБЛ., Г. ИВАНОВО, УЛ. ЖИДЕЛЕВА, Д. 19
УЧРЕДИТЕЛЬ: ВАЛЬЦЕВ СЕРГЕЙ ВИТАЛЬЕВИЧ

ИЗДАТЕЛЬСТВО «НАУЧНЫЕ ПУБЛИКАЦИИ»
HTTPS://SCIENTIFICPUBLICATIONS.RU
EMAIL: INFO@SCIENTIFICPUBLICATIONS.RU

РОСКОМНАДЗОР
СВИДЕТЕЛЬСТВО ЭЛ № ФС 77–65699

INTERNATIONAL STANDARD
SERIAL NUMBER 2542-081X

ЦЕНА СВОБОДНАЯ