XXVIIII Международной научно-практической конференции
«Актуальные проблемы науки и образования в условиях современных вызовов»

Исторический парк «Россия – моя история»;
Кыргызский национальный университет
им. Ж. Баласыгина;
ФГБОУ ВО «Российский государственный университет им. А.Н. Косыгина»;
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»;
ФГБОУ ВО «Уральский государственный аграрный университет»;
ФГБОУ ВО «Дагестанский государственный университет (филиал в г. Хасавюрте)»;
Образовательный холдинг «Институт развития образования и консалтинга»;
Финансово-экономический журнал

СБОРНИК МАТЕРИАЛОВ XVIII МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «РАЗВИТИЕ СОВРЕМЕННОЙ НАУКИ И ТЕХНОЛОГИЙ В УСЛОВИЯХ ТРАНСФОРМАЦИОННЫХ ПРОЦЕССОВ»

(шифр – МКНТ)

г. Москва, 01 марта 2024 г.

Москва – 2024

УДК 001
ББК 72
Р 34
DOI 10.34755/IROK.2024.39.15.019
ISBN 978-5-907769-37-3

«Актуальные проблемы науки и образования в условиях современных вызовов», **(2024, Москва)** / Сборник материалов XXVIIII Международной научно-практической конференции **– Санкт-Петербург: Изд-во «Печатный цех», 2024 –171с.**

В сборнике представлены материалы по актуальным проблемам науки и технологий, подготовленные участниками Международной научно-практической конференции «Развитие современной науки и технологий в условиях трансформационных процессов».
Материалы сборника охватывают широкий круг вопросов, содержат комплекс мер по решению актуальных проблем науки и технологий.
Сборник предназначен для научных и педагогических работников, преподавателей, аспирантов магистрантов и студентов с целью использования в научной работе и учебной деятельности.
Ответственность за аутентичность и точность цитат, имен, названий иных сведений, а также за соблюдение законов об интеллектуальной собственности несут авторы публикуемых материалов.
Сборник материалов конференции размещается в PDF на официальном сайте мероприятия http://www.f-ej.ru/Conferences# *, в Научной Электронной Библиотеке (eLibrary.ru) и индексируется в РИНЦ*

ISBN 978-5-907769-37-3
9 785907 769373

Основные направления конференции:

Биологические науки
Ветеринария
Военные науки
Географические науки
Геология
Информационные технологии
Искусствоведение
Исторические науки
Культурология
Лингвистика
Математические науки
Медицинские науки
Науки о Земле
Журналистика
Педагогические науки
Политические науки
Психологические науки
Сельскохозяйственные науки
Социологические науки
Технические науки
Туризм
Физические науки
Филологические науки
Философские науки
Химические науки
Экология и природопользование
Экономические науки
Этнография
Юридические науки.

Оглавление

Информационные технологии

Педагогические науки

Социологические науки

Экономические науки

Химические науки

Юридические науки

Информационные технологии

DOI 10.34755/IROK.2024.50.48.020

УДК 004.056.5

Горобей Ольга Владимировна

студент 4 курса направления «Информационная безопасность»
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»
Россия, г. Казань

Olga Vladimirovna Gorobey, 4th year student in the field of "Information Security"
FSBEI HE "Kazan National Research Technical University named after A.N. Tupolev-KAI"
Russia, Kazan

Описание техник проведения атаки Frankenstein в соответствии с матрицей MITRE ATT&CK

Description of Frankenstein attack techniques according to the MITRE ATT&CK matrix

Аннотация: в данной статье разобран механизм атаки Frankenstein (Франкенштейн), совершенной хакерской группировкой. Основной особенностью, примененной в описываемом случае, было использование нескольких компонентов в составе одного решения. Все эти компоненты имели открытый исходный код. Использованные злоумышленниками техники атаки были определены и описаны на основании данных, собранных

MITRE ATT&CK. Помимо возможного вреда, наносимого совершением атак, выявлены возможные способы извлечения пользы от использования и подробного изучения вредоносного программного обеспечения и методов совершения атак. Работа в указанного направлении была намечена в Техасском университете в Далласе.
Ключевые слова: MITRE ATT&CK, Frankenstein, компоненты с открытым кодом, техника атаки, злоумышленник.
Annotation: in this article, the mechanism of the Frankenstein attack by a hacker group is analyzed. The main feature used in the described case was the use of several components as part of a single solution. All of these components were open source. The attack techniques used by the attackers were identified and described based on data collected by MITRE ATT&CK. In addition to the potential harm caused by the attacks, possible ways to benefit from the use and detailed understanding of the malware and attack techniques were identified. Work in this area has been identified at the University of Texas at Dallas.
Key words: В 2019 году экспертами в области безопасности была обнаружена серия целенаправленных атак.

Была отслежена хакерская группировка, которая совершила несколько атак с января по апрель 2019 года, используя механизм Frankenstein (Франкенштейн). Целью атак было получение учетных данных жертв [1].

Примечательным было то, что инструменты, используемые хакерской группировкой создавались путем объединения четырех различных компонентов с открытом кодом:

1. Элемент article для определения, запущен ли образец на виртуальной машине;
2. GitHub-проект, использующий MSbuild , для выполнения команд PowerShell;
3. Компонент GitHub-проекта под названием Fruityc2 для создания стейджера;
4. GitHub-проект под названием PowerShell Empire для агентов [2].

Согласно классификации MITRE ATT&CK, данный инцидент относится к сфере атак на промышленные системы управления, ICS [3].

Рассмотрим основные техники, использованные при совершении атаки согласно данным MITRE ATT&CK [4] в таблице 1.

Таблица 1

Этапы атаки	Использованная техника	Описание техники
Resource Development (получение ресурсов)	Obtain Capabilities: Tool (Получение возможностей: Инструмент)	Участники группировкиполучили и использовали Empire, кроссплатформенный фреймворк с открытым исходным кодом,

Этапы атаки	Использованная техника	Описание техники
		доступный на GitHub. С его помощью злоумышленники получали возможность удаленного администрирования.
Initial Access (начальный доступ)	Phishing: Spearphishing Attachment (Фишинг: вложение для спирфишинга)	Далее злоумышленники применили методы социальной инженерии, а именно фишинг. Таким образом они рассылали электронные письма, содержащие вредоносные документы Microsoft Word.
Execution (исполнение)	Command and Scripting Interpreter: PowerShell (Интерпретатор команд и сценариев: PowerShell)	Участники группировки использовали PowerShell для запуска серии команд в кодировке Base64, которые выполняли роль промежуточного звена и перечисляли хосты, далее они запустили командный скрипт для настройки сохранения в виде запланированной задачи с именем "WinUpdate", а также другие закодированные команды из командной строки и использовали документы Word, которые побуждали жертву включить макросы и запустить скрипт Visual Basic. Они установили
	Command and Scripting Interpreter: Windows Command Shell (Командный и скриптовый интерпретатор: Командная оболочка Windows)	
	Command and Scripting Interpreter: Visual Basic (Интерпретатор команд и сценариев: Visual Basic)	
	Exploitation for Client Execution (Эксплуатация для выполнения клиента)	
	User Execution: Malicious File (Выполнение пользователем: Вредоносный файл)	
	Scheduled Task/Job: Scheduled Task (Запланированная задача/задание: Запланированная задача)	
	Windows Management Instrumentation	

Этапы атаки	Использованная техника	Описание техники
	(Инструментарий управления Windows)	сохранность состояния с помощью запланированной задачи, используя команду: /Create /F /SC DAILY /ST 09:00 /TN WinUpdate /TR, названной "WinUpdate", также использовали CVE-2017-11882 для выполнения кода на компьютере жертвы. И использовали запросы WMI для проверки того, запущены ли различные приложения безопасности, а также для определения версии операционной системы.
Defense Evasion (Уклонение от защиты)	Deobfuscate/Decode Files or Information (Деобфускация/декодирование файлов или информации)	Выполнение действий, описанных на предыдущем этапе оказалось возможным благодаря применению различных способов уклонения от защиты, таких как переименование вредоносных запланированных задач для имитации безопасной задачи, деобфускации команд, запуску закодированных команд из командной строки, использованию троянских документов и многим другим.
	Masquerading: Masquerade Task or Service (Маскарад: Маскировка задачи или услуги)	
	Obfuscated Files or Information: Command Obfuscation (Обфусцированные файлы или информация: Обфускация команд)	
	Template Injection (Инъекция шаблонов)	
	Trusted Developer Utilities Proxy Execution: MSBuild (Выполнение прокси-сервера Trusted Developer Utilities: MSBuild)	
Discovery (обнаружение)	Process Discovery (Обнаружение процесса)	Для обнаружения запущенных процессов

Этапы атаки	Использованная техника	Описание техники
	Software Discovery: Security Software Discovery (Обнаружение программного обеспечения: Обнаружение программного обеспечения для обеспечения безопасности)	использовался Empire, для обнаружение запущенных инструментов анализа в скомпрометированной системе использовались WMI
	System Information Discovery (Обнаружение системной информации)	
	System Network Configuration Discovery (Обнаружение конфигурации сети системы)	
	System Owner/User Discovery (Обнаружение владельца/пользователя системы)	
	Virtualization/Sandbox Evasion: System Checks (Виртуализация / Уклонение от песочницы: Проверки системы)	
Collection (сбор данных)	Automated Collection (Автоматизированная коллекция)	На данном этапе Empire автоматически собирал имена пользователя, домена, имени компьютера и другой системной информации.
	Data from Local System (Данные из локальной системы)	
Command and Control (командование и контроль)	Data from Local System (Данные из локальной системы)	Участники группировки использовали HTTP GET-запросы для C2 (командно-контрольный сервер).
	Encrypted Channel: Symmetric Cryptography (Зашифрованный канал: Симметричная криптография)	
	Ingress Tool Transfer (Передача инструмента для проникновения)	
Exfiltration (Эксфильтрация)	Automated Exfiltration (Автоматизированная эксфильтрация)	Информация собиралась через Empire, которая отправляла данные
	Exfiltration Over C2 Channel	

Этапы атаки	Использованная техника	Описание техники
	(Эксфильтрация по каналу C2)	обратно на C2 противника.

Но тем не менее данная разработка может оказаться полезной и для обеспечения безопасности. Так в Техасском университете в Далласе разработали схожий вирус, но применяться он должен не для нанесения ущерба, а для улучшения средств защиты [5].

Ключевая особенность «Франкенштейна» в том, что сборка рабочего тела по заданным инструкциям повторяется на каждом заражённом компьютере, но каждый раз задействуются новые гаджеты, так что бинарный файл вируса в каждом случае получается уникальным. За счёт этой особенности вредоносную программу практически невозможно обнаружить по базе вирусных сигнатур [6].

Таким образом можно сделать вывод, что детальное исследование средств, используемых злоумышленниками, может позволить улучшать средства защиты и, возможно, предупредить будущие угрозы.

Библиографический список:

1. Attackers Stitch Together Frankenstein Campaign Using Free Tools: [Электронный ресурс]. Режим доступа: https://www.bleepingcomputer.com/news/security/attackers-stitch-together-frankenstein-campaign-using-free-tools/. Дата обращения к ресурсу [28.02.2024].
2. Киберпреступники «собрали» операцию Frankenstein из разрозненных компонентов: [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/499360.php. Дата обращения к ресурсу [28.02.2024].
3. ICS Matrix: [Электронный ресурс]. Режим доступа: https://attack.mitre.org/matrices/ics/. Дата обращения к ресурсу [28.02.2024].
4. Frankenstein: [Электронный ресурс]. Режим доступа: https://attack.mitre.org/campaigns/C0001/. Дата обращения к ресурсу [28.02.2024].
5. Вирус Frankenstein заимствует код у других программ: [Электронный ресурс]. Режим доступа: https://xakep.ru/2012/08/20/59187/. Дата обращения к ресурсу [28.02.2024].
6. 'Frankenstein' computer program created: [Электронный ресурс]. Режим доступа: https://www.upi.com/Science_News/Technology/2012/08/28/Frankenstein-

computer-program-created/55421346189707/. Дата обращения к ресурсу [28.02.2024].

0УДК 004.5

Лукьянов Эмиль Радикович
студент
Шарипов Рифат Рашатович, научный руководитель,
доцент кафедры «Систем информационной безопасности»
Казанский национальный исследовательский технический университет
им. А.Н. Туполева-КАИ
lukanovemil6@gmail.com
Россия, г. Казань

Lukyanov Emil Radikovich
student
Rifat Rasatovich Sharipov, scientific supervisor,
Associate Professor of the Department of Information Security Systems
Kazan National Research Technical University named after. A.N. Tupolev-KAI
lukanovemil6@gmail.com
Russia, Kazan

Обзор и рекомендации NGFW

NGFW overview and recommendations

Аннотация: Данная научная статья представляет собой подробный обзор и анализ межсетевого экрана нового поколения (NGFW). Исследование, нацелено на обзор межсетевого экрана нового поколения, а

также рекомендации к его применению. Рассматриваются актуальные вопросы защиты информации используемые при создании таких программно-аппаратных элементов компьютерной сети. Предоставляются подробный состав оборудования используемый для межсетевого экрана нового поколения в компании.

Ключевые слова: межсетевой экран нового поколения, защита информации.

Abstract: This research paper presents a comprehensive overview and analysis of the Next-Generation Firewall (NGFW). The study aims to provide an in-depth understanding of NGFW, their applications, and recommendations for their implementation. It examines the current trends and challenges in cybersecurity that have driven the development of NGFWs. The paper also provides a detailed breakdown of the hardware and software components used in NGFW, along with their functionalities and benefits. The research findings offer valuable insights and recommendations for organizations looking to enhance their network security posture by deploying NGFW.

Key words: NGFW, information protection.

NGFW (Next Generation Firewall) — межсетевой экран нового поколения предназначенный для глубокой фильтрации трафика, интегрированный с IDS (Intrusion Detection System, система обнаружения вторжений) или IPS (Intrusion Prevention System, система предотвращения вторжений) и обладающий возможностью контролировать и блокировать трафик на уровне приложений.

Основная цель межсетевого экрана нового поколения (NGFW) заключается в обеспечении более эффективной защиты компьютерных сетей от различных угроз и атак. NGFW представляет собой развитие традиционных межсетевых экранов, добавляющее дополнительные функции и возможности.

Основные характеристики NGFW включают в себя:

1. Проверка пакетов на уровне приложений: NGFW способен анализировать сетевой трафик на уровне приложений, что позволяет обнаруживать и блокировать угрозы, которые могут скрываться внутри сетевых протоколов.

2. Межсетевой экран нового поколения может работать совместно системой предотвращения вторжений (IPS) которая позволяет обнаруживать и блокировать попытки вторжения в реальном времени.

3. Управление доступом: NGFW предоставляет возможность управления доступом к сети, определяя политики доступа на основе различных параметров, таких как пользователи, группы пользователей, приложения и т.д.

4. VPN-сервер: NGFW может служить в качестве VPN-сервера, обеспечивая защищенное удаленное подключение к сети.

5. Отчетность и мониторинг: NGFW предоставляет возможность анализа и мониторинга сетевого трафика, а также создания отчетов о событиях и угрозах.

В Российской Федерации существуют несколько законов, а также стандартов, которые регулируют область информационной безопасности и могут быть применимы к межсетевым экранам нового поколения (NGFW). Некоторые из них включают:

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" (№ 149-ФЗ).
2. Федеральный закон "О связи" (№ 126-ФЗ).
3. ГОСТ Р ИСО/МЭК 27001-2013.
4. ГОСТ Р ИСО/МЭК 15408-2019.
5. ГОСТ Р 34.10-2012.

Существует множество законов и стандартов, которые могут быть применимы к межсетевым экранам нового поколения в Российской Федерации. Однако стоит отметить, что требования могут различаться в зависимости от конкретной отрасли в которой функционирует организация. Все эти меры помогут укрепить безопасность и повысить осведомленность сотрудников о социальной инженерии. Однако важно помнить, что безопасность является непрерывным процессом, и регулярное обновление и адаптация мер безопасности являются неотъемлемой частью защиты от новых угроз.

Эффективное противодействие социальной инженерии требует комплексного подхода, включающего в себя как организационные, так и технические меры безопасности. С учетом динамичности киберугроз и постоянного развития новых методов, построение безопасности и постоянное обучение персонала остаются ключевыми компонентами в обеспечении информационной безопасности.

Для монтирования межсетевого экрана нового поколения (NGFW) требуется определенный набор оборудования. Вот основные элементы, которые могут входить в такую конфигурацию:

- Межсетевой экран нового поколения (NGFW): это основное устройство, выполняющее функции анализа и фильтрации сетевого трафика, обнаружения и блокирования угроз, а также управления доступом к сети. NGFW обычно представляет собой аппаратное устройство или программное решение, способное обрабатывать большие объемы трафика и обеспечивать высокую производительность.
- Коммутаторы (Switches): Коммутаторы используются для создания сетевой инфраструктуры и обеспечения соединения между

устройствами в сети. Они позволяют передавать трафик между различными портами и устройствами, включая межсетевой экран.

- Маршрутизаторы (Routers): Маршрутизаторы отвечают за передачу данных между различными сетями и определение оптимального пути для доставки пакетов данных.
- Серверы: Серверы могут быть использованы для внедрения дополнительных функций, таких как системы предотвращения вторжений (IPS), системы обнаружения вторжений (IDS), системы аналитики и управления. Они могут взаимодействовать вместе с межсетевым экраном для обеспечения более широкого спектра защиты и анализа сети.
- Кабели и сетевое оборудование: для обеспечения связи между устройствами в сети требуются соответствующие сетевые кабели, разъемы и другое сетевое оборудование, такое как патч-панели и розетки.
- Источники питания и резервное питание: для обеспечения бесперебойной работы межсетевого экрана и других устройств рекомендуется использовать надежные источники питания, а также резервные источники питания (UPS) для защиты от сбоев в электроснабжении и непредвиденных сбоев в электроснабжении они могут привести к потере данных, нарушению работы сети и уязвимости для кибератак.

В зависимости от конкретных потребностей и конфигурации сети, комплект оборудования для подключения NGFW может различаться. Рекомендуется обратиться к документации и руководству по установке и настройке конкретной модели NGFW для получения более подробной информации.

Для достижения правильной установки межсетевого экрана нового поколения (NGFW) рекомендуется следовать нескольким рекомендациям, чтобы обеспечить правильную настройку и эффективную работу устройства. Вот некоторые из них:

1. Планирование и анализ сети: перед установкой NGFW рекомендуется провести тщательное планирование и анализ сети. Важно определить основные цели и требования безопасности, изучить текущую сетевую инфраструктуру, определить основные потоки трафика и выделить наиболее критические зоны сети.

2. Правильное размещение: Размещение NGFW в сети играет важное значение. Рекомендуется размещать NGFW на границе сети, между внутренней и внешней сетями, чтобы обеспечить контроль и фильтрацию всего трафика, проходящего через границу. Необходимо учесть физическую безопасность устройства и обеспечьте его защиту от несанкционированного доступа.

3. Обновление программного обеспечения: убедитесь, что вы используете последнюю версию программного обеспечения для NGFW.

Регулярно проводите обновления устройства, чтобы получить новые функции, исправления ошибок и обновления безопасности. Это поможет защитить вашу сеть от новых угроз и эксплойтов.

4. Настройка правил безопасности: Правильная настройка правил безопасности является ключевым фактором работы NGFW. Необходимо определить политики безопасности, опираясь на требования и цели. Создать правила фильтрации трафика, управления доступом, блокировки угроз и другие необходимые правила. Регулярно обновляйте и проводите аудит, чтобы гарантировать их актуальность и эффективность.

5. Мониторинг и анализ: не забывайте настраивать мониторинг и анализ работы NGFW. Включите журналирование событий и уведомления о нарушениях безопасности. Регулярно проверяйте журналы и анализируйте данные, чтобы обнаруживать и реагировать на потенциальные угрозы и атаки.

6. Обучение и обновление навыков: постоянно развивайте свои навыки и знания в области NGFW и информационной безопасности. Следите за новыми угрозами и тенденциями, участвуйте в тренингах и сертификационных программах, чтобы быть в курсе последних разработок и лучших практик.

Установка NGFW требует внимательности и планирования. Если у вас есть специфические требования или особенности сети, рекомендуется проконсультироваться с поставщиком NGFW или обратиться к специалистам по информационной безопасности для получения дополнительной помощи и рекомендаций.

Заключение. Данная научная статья представляет собой подробный обзор и анализ межсетевого экрана нового поколения (NGFW) который играет ключевую роль в обеспечении безопасности современных компьютерных сетей. Он представляет собой новый этап эволюции традиционных брандмауэров, обладая дополнительными функциями, такими как глубокий анализ трафика, контроль приложений и защита от усовершенствованных атак. Необходимо подчеркнуть важность проведения тщательного планирования и анализа сети перед установкой NGFW является ключевым шагом. Определение целей безопасности, изучение инфраструктуры, анализ потоков трафика и выделение критических зон сети помогают определить оптимальное размещение и конфигурацию устройства. Размещение NGFW на границе сети обеспечивает контроль трафика между внутренней и внешней сетями, обеспечивая физическую безопасность и защиту от несанкционированного доступа. Проведение анализа сети перед установкой NGFW позволяет эффективно защитить сеть и данные, определить оптимальное место для установки устройства и настроить его конфигурацию с учетом особенностей сети. Таким образом, межсетевые экраны нового поколения (NGFW) являются важной частью современных

систем безопасности, обеспечивая эффективный контроль трафика, защиту от угроз и атак, а также обеспечивая целостность и конфиденциальность данных в сети.

Библиографический список:

1. Лукьянов Э. Р. Разработка системы контроля управления доступом в компании Арсенал // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XXV Международной научно-практической конференции, Москва, 17 ноября 2023 года. –Москва. Печатный цех, 2023 – С. 202-208.

2. Шарипов, Р. Р. Исследования скорости передачи данных в PLC сети в учебной лаборатории / Р. Р. Шарипов, А. Ф. Фатхелисламов // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 55-60.

3. Шарипов, Р. Р. Исследование электрических параметров пороговых извещателей / Р. Р. Шарипов, Б. З. Юсупов // Программные системы и вычислительные методы. – 2023. – № 3. – С. 29-47. – DOI 10.7256/2454-0714.2023.3.43682.

4. Юсупов, Б. З. Разработка учебного стенда охранно-пожарной системы для обучения студентов / Б. З. Юсупов // Программные системы и вычислительные методы. – 2023. – № 2. – С. 40-48. – DOI 10.7256/2454-0714.2023.2.43552.

5. Юсупов, Б. З. Методика проведения лабораторных работ на стенде «ОПС Астра-812pro» по дисциплине «Технические средства охраны» / Б. З. Юсупов, А. М. Мартынов, Р. Р. Шарипов // Информационные технологии в науке, промышленности и образовании. Молодежный научный форум: Сборник трудов Всероссийской научно-технической конференции, Ижевск, 25–26 мая 2023 года. – Ижевск: Ижевский государственный технический университет имени М.Т. Калашникова, 2023.

6. Мартынов, А. М. Разработка учебного стенда системы видео контроля / А. М. Мартынов // Программные системы и вычислительные методы. – 2023. – № 4. – С. 102-114. – DOI 10.7256/2454-0714.2023.4.69055.

0УДК 004.5

Лукьянов Эмиль Радикович, студент
Степанов Максим Олегович, студент
Мисбахов Нияз Ильясович, студент
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ
Россия, г. Казань

Шарипов Рифат Рашатович, научный руководитель,
доцент кафедры «Систем информационной безопасности»
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ
Россия, г. Казань

Lukyanov Emil Radikovich, student
Stepanov Maxim Olegovich, student
Misbakhov Niyaz Ilyasovich, student
Kazan National Research Technical University named after. A.N. Tupolev-KAI

Russia, Kazan

Rifat Rasatovich Sharipov, scientific supervisor,
Associate Professor of the Department of Information Security Systems
Kazan National Research Technical University named after. A.N. Tupolev-KAI
Russia, Kazan

Обзор Программно-аппаратного комплекса (ПАК) «Соболь»

Review of the Software and Hardware Complex (SHC) «Sable»

Аннотация: Статья представляет обзор программно-аппаратного комплекса "Соболь", который спроектирован для защиты компьютера от несанкционированного доступа. В статье рассматривается, как может поставляться комплекс, его ключевые характеристики и возможности. Рассматривается принцип работы, а также иллюстрируется внешний вид платы. В статье приведены рекомендации при установке Программно-аппаратного комплекса "Соболь" также важность этого комплекса для повышения эффективности работы в современных условиях и обсуждают перспективы его будущего развития.
Ключевые слова: Программно-аппаратного комплекса, защита информации.
Abstract: The article presents an overview of the Sobol software and hardware complex, which is designed to protect a computer from unauthorized access. The article discusses how the complex can be delivered, its key characteristics and capabilities. The principle of operation is considered, and the appearance of the board is illustrated. The article provides recommendations for installing the Sobol software and hardware complex, as well as the importance of this complex for improving work efficiency in modern conditions and discusses the prospects for its future development.
Key words: Hardware and software complex, information protection.

ПАК Соболь (Программно-аппаратный комплекс "Соболь") — это российская разработка в области информационной безопасности. Этот комплекс предназначен для обеспечения защиты информации от утечек и несанкционированного доступа. ПАК Соболь включает в себя как программное, так и аппаратное обеспечение, которые работают совместно для обеспечения безопасности данных.

Состав ПАК "Соболь" может включать в себя следующие компоненты:

Аппаратная часть:

- Компьютерное оборудование (компьютеры, серверы и т. д.).
- Устройства сбора данных (датчики, измерительные приборы и т. д.).
- Устройства управления (реле, приводы и т. д.).

2. Программное обеспечение:
- Операционная система.
- Специализированные программы для управления процессами.
- Программы для обработки и анализа данных.
- Программы визуализации данных.

3. Сетевое оборудование: Средства связи для передачи данных между компонентами системы.

4. Интерфейсы:
- Графический интерфейс пользователя.
- Интерфейсы для взаимодействия с внешними устройствами.

5. Хранение данных: Базы данных для хранения информации о процессах и результатах измерений.

Это общий обзор типичных компонентов, которые могут входить в состав программно-аппаратного комплекса "Соболь". Конкретный состав может различаться в зависимости от конкретного применения и требований заказчика. Общая цель ПАК "Соболь" - обеспечить защиту информации от несанкционированного доступа через радиоканалы.

Комплекс "Соболь" реализует следующие основные функции:

• идентификация и аутентификация пользователей компьютера при входе в

информационную систему с помощью электронных идентификаторов;

• защита от несанкционированной загрузки операционной системы со съемных носителей;

• контроль целостности (КЦ) программного и аппаратного обеспечения защищаемого компьютера до загрузки операционной системы;

• сторожевой таймер — блокировка компьютера при условии, что после его включения управление не передано расширению UEFI/BIOS комплекса;

• контроль работоспособности датчика случайных чисел, энергонезависимой памяти платы комплекса, персональных идентификаторов;

• регистрация событий, имеющих отношение к безопасности информационной системы.

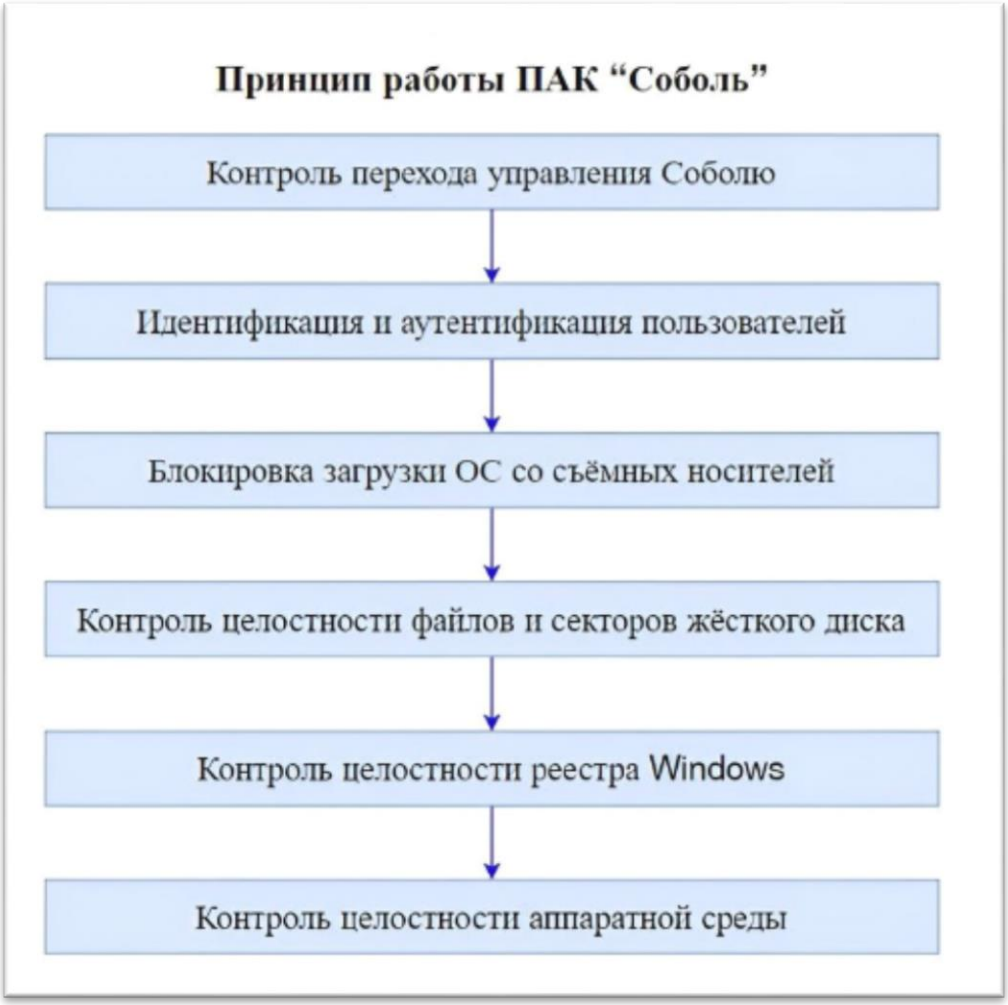


Рисунок 1. – Принцип работы ПАК «Соболь»

Поставка плат происходит в двух вариантах в зависимости от используемого ДСЧ (Датчик случайных чисел)

Вариант платы	ДСЧ
PCIe (вариант 1)	Контролируемый двухканальный аппаратный ДСЧ
Mini PCIe Half (вариант 1)	
M.2 (вариант 1)	
PCIe (вариант 2)	Программный ДСЧ
Mini PCIe Half (вариант 2)	
M.2 (вариант 2)	

Табл.1. Варианты плат ПАК «Соболь»

Рассмотрим плату ПАК Соболь Версия 4. Она может быть сертифицирован ФСТЭК, ФСБ, МО или ФСТЭК+ФСБ на выбор. Далее представлен внешний вид платы:

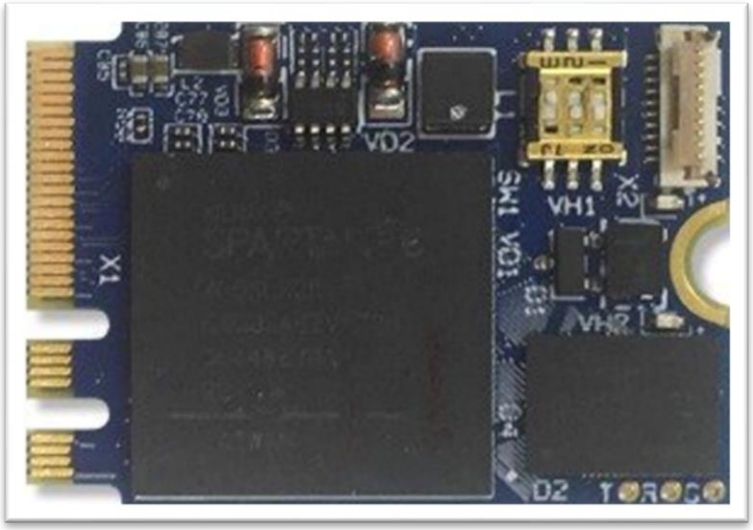


Рисунок 2. - Плата ПАК «Соболь»

При установке Программно-аппаратного комплекса (ПАК) "Соболь" рекомендуется следовать следующим рекомендациям:

- Подготовьте необходимое оборудование: убедитесь, что у вас есть все необходимое оборудование для установки ПАК "Соболь". Это может включать в себя компьютеры, серверы, сетевое оборудование и другие компоненты.
- Проверьте системные требования: убедитесь, что ваше оборудование соответствует системным требованиям ПАК "Соболь". Это поможет избежать проблем с производительностью и совместимостью.
- Создайте резервную копию данных: прежде чем начать установку, рекомендуется создать резервную копию всех важных данных на компьютере или сервере, чтобы в случае проблем можно было восстановить информацию.
- Следуйте инструкциям по установке: внимательно изучите инструкции по установке ПАК "Соболь" и следуйте им шаг за шагом. Не пропускайте никакие этапы установки.
- Обновляйте ПО: после установки убедитесь, что все программное обеспечение в ПАК "Соболь" обновлено до последних версий. Это поможет обеспечить безопасность и стабильную работу системы.
- Проведите тестирование: после установки ПАК "Соболь" рекомендуется провести тестирование системы, чтобы убедиться, что все работает правильно и без ошибок.
- Обучение персонала: Обеспечьте обучение сотрудников, которые будут использовать ПАК "Соболь", чтобы они могли эффективно работать с системой и использовать ее функционал на полную мощность.

- Обеспечьте безопасность: обратите особое внимание на безопасность при установке ПАК "Соболь". Убедитесь, что доступ к системе защищен паролями и другими методами аутентификации.

Следуя этим рекомендациям, вы сможете успешно установить и использовать Программно-аппаратный комплекс "Соболь" для своих потребностей.

Заключение. Продукт "Соболь" от компании "Код Безопасности" - передовое решение в области безопасности и контроля доступа, обладающее высокой функциональностью, надежностью и инновационными возможностями. Он широко популярен среди различных организаций и предприятий благодаря своей способности обеспечивать эффективное управление доступом, защиту конфиденциальных данных и обеспечение безопасности помещений. С использованием передовой технологии и возможностей интеграции, ПАК "Соболь" помогает организациям повысить уровень безопасности и эффективности операций, что делает его неотъемлемым инструментом для современных бизнес-сред.

Библиографический список:

1. Фаткулин, А. Н. Анализ современных систем контроля и управления доступом / А. Н. Фаткулин, Е. Н. Окладникова, Е. Н. Сухарев // Актуальные проблемы авиации и космонавтики. – 2011. – Т. 1, № 7. – С. 263-264.

2. Патент № 2643898 C1 Российская Федерация, МПК G07C 9/00. Система контроля и управления доступом с использованием мобильного телекоммуникационного устройства: № 2016145370: заявл. 18.11.2016: опубл. 06.02.2018 / Т. Ю. Шейкин.

3. Юсупов, Б. З. Разработка лабораторного стенда охранно-пожарной сигнализации по дисциплине технические средства охраны / Б. З. Юсупов, А. М. Мартынов // Актуальные проблемы науки и образования в условиях современных вызовов : Сборник материалов XIX Международной научно-практической конференции, Москва, 21 марта 2023 года. – Москва: Печатный цех, 2023. – С. 80-91.

4. Лукьянов, Э. Р. Разработка системы контроля управления доступом в компании Арсенал / Э. Р. Лукьянов // Актуальные проблемы науки и образования в условиях современных вызовов (шифр –МКАП 25): Сборник материалов XXV Международной научно-практической конференции, Москва, 17 ноября 2023 года. – Москва: Печатный цех, 2023. – С. 202-209. – EDN YCGPSQ.

5. Шарипов, Р. Р. Исследование электрических параметров пороговых извещателей / Р. Р. Шарипов, Б. З. Юсупов // Программные системы и вычислительные методы. – 2023. – № 3. – С. 29-47. – DOI 10.7256/2454-0714.2023.3.43682.

6. Юсупов, Б. З. Разработка учебного стенда охранно-пожарной системы для обучения студентов / Б. З. Юсупов // Программные системы и вычислительные методы. – 2023. – № 2. – С. 40-48. – DOI 10.7256/2454-0714.2023.2.43552.

7. Юсупов, Б. З. Методика проведения лабораторных работ на стенде «ОПС Астра-812pro» по дисциплине «Технические средства охраны» / Б. З. Юсупов, А. М. Мартынов, Р. Р. Шарипов // Информационные технологии в науке, промышленности и образовании. Молодежный научный форум: Сборник трудов Всероссийской научно-технической конференции, Ижевск, 25–26 мая 2023 года. – Ижевск: Ижевский государственный технический университет имени М.Т. Калашникова, 2023.

8. Мартынов, А. М. Разработка учебного стенда системы видео контроля / А. М. Мартынов // Программные системы и вычислительные методы. – 2023. – № 4. – С. 102-114. – DOI 10.7256/2454-0714.2023.4.69055.

9. Юсупов, Б. З. Методика проведения лабораторных работ на стенде «ОПС Астра-812pro» по дисциплине «Технические средства охраны» / Б. З. Юсупов, А. М. Мартынов, Р. Р. Шарипов // Информационные технологии в науке, промышленности и образовании. Молодежный научный форум: Сборник трудов Всероссийской научно-технической конференции, Ижевск, 25–26 мая 2023 года. – Ижевск: Ижевский государственный технический университет имени М.Т. Калашникова, 2023. – С. 476-479.

УДК 004.056

Лукьянов Эмиль Радикович, студент
Мисбахов Нияз Ильясович, студент
Степанов Максим Олегович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, Student
Lukyanov Emil Radikovich, Student
Misbachov Niaz Ilyasovich, Student
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI

Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer of the department "Si" "Information security system"
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI
Russland, Kasan

Обзор сетевых атак и методов их предотвращения на канальном уровне

Overview of network attacks and methods of preventing them at the channel level

Аннотация: В данной статье рассматривается канальный уровень сетевой модели OSI, его роль в обеспечении надежности и эффективности передачи данных в сети. Особое внимание уделяется потенциальным атакам, которые могут возникнуть на этом уровне, и стратегиям защиты от них. В тексте также акцентировано внимание на различных технологиях и подходах, которые могут быть использованы для обеспечения безопасности на канальном уровне.
Ключевые слова: канальный уровень, OSI, информационная безопасность, атаки.
Abstract: This article discusses the channel layer of the OSI network model, its role in ensuring the reliability and efficiency of data transmission in the network. Special attention is paid to potential attacks that may occur at this level and strategies to protect against them. The text also focuses on various technologies and approaches that can be used to ensure security at the channel level.
Keywords: channel layer, OSI, information security, attacks.

Канальный уровень (англ. Data Link layer), также уровень передачи данных, уровень звена данных — второй уровень сетевой модели OSI, предназначенный для передачи данных узлам, находящимся в том же сегменте локальной сети [1]. Этот уровень преобразует биты из физического уровня в структурированные блоки данных, известные как кадры, которые затем передаются дальше по сети. Основные функции канального уровня включают фрейминг, физическую адресацию, контроль потока, обнаружение и коррекцию ошибок, а также управление доступом к среде. Все эти функции обеспечивают надежность и эффективность передачи данных, делая канальный уровень неотъемлемым компонентом любой сети.

Однако, несмотря на все его преимущества, канальный уровень также подвержен различным типам атак, которые могут нарушить нормальную работу сети. Атаки могут быть использованы для нарушения целостности, доступности или конфиденциальности данных. Существует множество различных типов атак на канальном уровне, в том числе:

Атаки типа "отказ в обслуживании" (DoS):

Действия, направленные на перегрузку ресурсов целевого узла сети трафиком, с целью временного или постоянного лишения его возможности

обработки легитимных запросов, представляют собой DoS-атаки. В результате таких атак услуги или ресурсы, предоставляемые целевым узлом, становятся недоступными для других пользователей.

Злоумышленники используют разнообразные методы для создания значительного объема сетевого трафика. Это достигается через использование ботнетов (сетей зараженных компьютеров), распределенных сетей или других средств. После этого они направляют этот интенсивный трафик на целевой узел, перегружая его сетевые, вычислительные или иные ресурсы.

В результате избыточной нагрузки целевой узел сталкивается с временным или постоянным отказом в обслуживании. Это выражается в недоступности для легитимных пользователей услуг, предоставляемых узлом, таких как веб-сайты, серверы или другие сетевые службы.

Атаки типа "спуфинг" (подмена):

Спуфинг (от английского слова spoofing) - это кибер-атака, в рамках которой мошенник выдает себя за какой-либо надежный источник, чтобы получить доступ к важным данным или информации [2]. В результате целевой узел может взаимодействовать с поддельным узлом, полагая, что это легитимное общение.

Злоумышленники посылают в сеть ложные пакеты данных, изменяя различные идентификационные параметры, такие как MAC-адреса или другие сетевые атрибуты. Целевой узел получает эти ложные данные и идентифицирует отправителя как легитимный узел. Это может привести к тому, что целевой узел доверяет поддельному узлу, считая его частью доверенной сети. Злоумышленники, внедрившись в сеть, могут манипулировать обменом данными между целевым и другими узлами, что может включать в себя перехват, модификацию или даже блокирование данных.

Атаки типа "перехват трафика" (sniffing):

Атаки перехвата трафика представляют собой стратегии, нацеленные на перехват и мониторинг сетевого трафика, передаваемого между двумя узлами. Основная цель таких атак состоит в том, чтобы получить несанкционированный доступ к данным, передаваемым по сети, с возможностью просмотра и анализа этой информации.

Злоумышленники используют специальные инструменты или программное обеспечение для отслеживания и захвата трафика в сети. Атакующие перехватывают сетевые пакеты данных, содержащие информацию, передаваемую между узлами. Далее, производят анализ перехваченных данных с целью извлечения чувствительной информации, такой как логины, пароли, или другие конфиденциальные данные.

Атаки типа "отравление ARP" (ARP poisoning):

Атаки отравления ARP представляют собой стратегии, направленные на изменение таблицы ARP (Address Resolution Protocol) целевого узла в сети. Целью таких атак является введение в заблуждение сетевых устройств относительно соответствия IP-адресов и MAC-адресов, что может привести к перенаправлению трафика на неправильный узел.

Злоумышленники отправляют ARP-пакеты в сеть, содержащие ложные соответствия между IP-адресами и MAC-адресами. Когда устройства в сети получают эти ложные ARP-пакеты, они обновляют свои таблицы ARP, считая, что указанный IP-адрес соответствует указанному MAC-адресу. Это приводит к тому, что трафик, предназначенный для определенного IP-адреса, направляется на поддельный MAC-адрес, контролируемый злоумышленниками.

Например, если злоумышленник желает перехватывать трафик между компьютером A и маршрутизатором, он может отправить ложные ARP-пакеты, указывая, что его MAC-адрес является "правильным" MAC-адресом маршрутизатора для IP-адреса компьютера A, и наоборот. Таким образом, весь трафик, который должен был бы направляться непосредственно между компьютером A и маршрутизатором, будет проходить через злоумышленника.

Атаки типа "атака на MAC-адрес" (MAC flooding):

Атаки MAC Flooding представляют собой методы, направленные на переполнение таблицы MAC-адресов сетевого устройства. Основная цель таких атак заключается в создании перегрузки таблицы MAC-адресов устройства, что может привести к его временному или постоянному отказу в обработке сетевого трафика.

Злоумышленники могут перегрузить таблицу MAC-адресов целевого устройства, генерируя и отправляя в сеть большое количество кадров данных, каждый с уникальным поддельным MAC-адресом. Поскольку таблица имеет ограниченный размер, при продолжительной атаке она может быть заполнена, что приведёт к переполнению.

В результате, когда устройство пытается найти реальные MAC-адреса узлов в сети, оно сталкивается с перегруженной таблицей. Это может замедлить или полностью остановить его способность эффективно обрабатывать новый трафик, что приведёт к нарушению работы сети.

Анализируя спектр атак на канальном уровне, становится очевидной их потенциальная опасность для стабильности и безопасности сетевых систем. Эти атаки могут вызвать значительные нарушения в функционировании сети, привести к утечке конфиденциальной информации и даже к полному отказу обслуживания. Особую сложность представляет то, что они осуществляются на низком уровне, где стандартные меры безопасности могут оказаться неэффективными.

Вместе с тем, несмотря на высокую степень угрозы, необходимо подчеркнуть, что существуют методы и технологии, разработанные специально для противодействия атакам на канальном уровне. Эти инструменты позволяют специалистам по сетевой безопасности эффективно противодействовать потенциальным угрозам и обеспечивать стабильность сетевых систем.

Рассмотрим несколько подходов, которые могут быть применены для эффективной защиты сети от атак на канальном уровне.

MAC-фильтрация является одним из методов защиты на канальном уровне. Это процесс, в котором коммутаторы или беспроводные точки доступа используются для блокировки или разрешения сетевого доступа на основе MAC-адреса устройства. Это может помочь предотвратить несанкционированный доступ к сети.

Применение технологии виртуальных локальных сетей (VLAN) на канальном уровне позволяет эффективно разделять физическую сетевую инфраструктуру на отдельные логические сегменты. Этот метод создает виртуальные границы, которые предотвращают взаимодействие между устройствами, находящимися в разных виртуальных сегментах. Более того, эта технология упрощает управление безопасностью, позволяя администраторам гибко настраивать и контролировать политики безопасности для каждого виртуального сегмента независимо. Такой подход обеспечивает высокую степень гибкости и эффективности при управлении сетью на канальном уровне.

Протокол аутентификации IEEE 802.1X предоставляет механизм проверки подлинности устройств перед предоставлением им доступа к сети. В процессе аутентификации участвуют supplicant (устройство, запрашивающее доступ), authenticator (сетевое устройство, контролирующее доступ) и authentication server (сервер аутентификации). При подключении устройства к сети, оно отправляет запрос на аутентификацию. Authenticator блокирует весь трафик, кроме специального трафика аутентификации. Supplicant предоставляет свои учетные данные через протокол EAPOL, а Authenticator передает их серверу аутентификации для проверки. Если учетные данные верны, устройству разрешается доступ, и трафик становится разрешенным. IEEE 802.1X обеспечивает различные методы аутентификации, включая использование сертификатов.

На канальном уровне используют протоколы VPN, которые создают защищенные туннели для передачи данных между устройствами. Два основных протокола для канального уровня VPN - это PPTP и L2TP.

PPTP (Point-to-Point Tunneling Protocol) предоставляет базовое шифрование для обеспечения конфиденциальности данных. Он прост в настройке и обеспечивает быструю передачу данных, но считается менее безопасным из-за ограниченных методов шифрования.

L2TP (Layer 2 Tunneling Protocol) сам по себе не обеспечивает шифрование, но обычно используется в сочетании с протоколом IPsec (IP Security) для обеспечения безопасности данных. L2TP/IPsec обеспечивает более высокий уровень безопасности по сравнению с PPTP за счет более сложного процесса шифрования.

Другие протоколы VPN на канальном уровне включают OpenVPN, IKEv2 (Internet Key Exchange version 2)

OpenVPN - это протокол VPN с открытым исходным кодом, предоставляющий надежную безопасность передаваемых данных и возможности гибкой настройки. Он использует разнообразные алгоритмы шифрования и аутентификации, что позволяет настроить уровень безопасности в соответствии с конкретными требованиями.

IKEv2 - это протокол VPN, который обеспечивает безопасный обмен ключами и аутентификацию между устройствами. Он часто используется в сочетании с IPsec для создания защищенных VPN-туннелей. IKEv2 обеспечивает высокую производительность и быструю переподключаемость при переходе между различными сетевыми средами, обеспечивая при этом защиту данных.

Внедрение современных технологий, таких как искусственный интеллект и машинное обучение, может помочь в автоматизации процессов обнаружения и предотвращения атак на канальном уровне. Эти технологии могут анализировать большие объемы данных в режиме реального времени и выявлять аномалии, которые могут указывать на наличие атаки.

Заключение. Канальный уровень, играет критическую роль в общей структуре сетевой безопасности. Атаки на этом уровне представляют серьезную угрозу, так как они могут нарушить целостность, доступность и конфиденциальность данных. Несмотря на его невидимость для конечного пользователя, канальный уровень сети является фундаментом, на котором строится вся сеть. Неправильная или недостаточная защита этого уровня может привести к серьезным последствиям, включая потерю данных, нарушение работы сети и уязвимость перед атаками. Поэтому администраторам сетей крайне важно уделить должное внимание защите низшего уровня сети, используя все доступные методы и технологии.

Библиографический список:

1. Канальный уровень: [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Канальный_уровень (Дата обращения: 20.01.2024)
2. Что такое спуфинг и как предотвратить спуфинг-атаку: [Электронный ресурс]. URL:

https://www.securitylab.ru/blog/company/pandasecurityrus/350091.php?ref=123 (Дата обращения: 20.01.2024)
3. Отравление ARP: что это такое и как предотвратить ARP-спуфинг: [Электронный ресурс]. URL: https://habr.com/ru/companies/varonis/articles/562144/ (Дата обращения: 20.01.2024)
4. MAC flooding: [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/MAC_flooding (Дата обращения: 20.01.2024)
5. Использование стандарта IEEE 802.1x в сети передачи данных: [Электронный ресурс]. URL: https://habr.com/ru/articles/138889/ (Дата обращения: 20.01.2024)

УДК 004.056.53

Мисбахов Нияз Ильясович

студент
Ахметвалеев Амир Муратович,
научный руководитель, кандидат технических наук, доцент кафедры «Систем информационной безопасности»

Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ
Россия, г. Казань

Misbakhov Niyaz Ilyasovich
student
Akhmetvaleev Amir Muratovich
scientific supervisor, candidate of technical sciences, associate professor of the department of "Information Security Systems"
Kazan National Research Technical University named after. A.N. Tupolev-KAI
Russia, Kazan

Исследование методов эксплуатации уязвимости SSTI

Research on methods for exploiting the SSTI vulnerability

Аннотация: В данной статье анализируется уязвимость SSTI в контексте безопасности систем, использующих шаблонизаторы. Описаны применение и цели шаблонизаторов, приведены схемы работы. Рассмотрены причины возникновения SSTI, потенциальные последствия эксплуатации данной уязвимости и меры защиты. Приведены способы обнаружения этой уязвимости и указаны практические реализации этой атаки с повышением критичности до чтения локального файла из сервера и удаленного выполнения команд.

Ключевые слова: SSTI, веб-приложение, уязвимость, шаблонизатор, информационная безопасность.

Annotation: This article analyzes the SSTI vulnerability in the context of the security of systems using template engines. The application and goals of template engines are described, and operation schemes are given. The causes of SSTI, the potential consequences of exploiting this vulnerability, and protective measures are considered. Methods for detecting this vulnerability are given and practical implementations of this attack are indicated with increasing criticality to reading a local file from the server and remotely executing commands.

Key words: SSTI, web application, vulnerability, template engine, information security.

Шаблонизатор - это инструмент, который позволяет упростить написание разметки, делить её на компоненты и связывать с данными. Главное преимущество шаблонизаторов - избавление от необходимости писать повторяющийся код несколько раз. Это кажется не такой большой проблемой, но всё же разработчикам часто приходится тратить на это время [1].

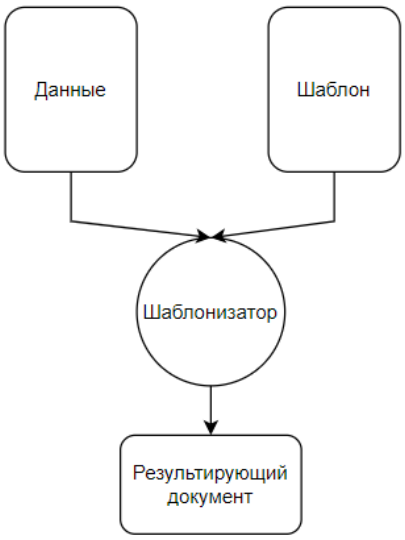


Рисунок 1 Схема работы шаблонизатора

Внедрение шаблона на стороне сервера (Server-Side Template Injection) - это когда злоумышленник может использовать собственный синтаксис шаблонизатора для внедрения вредоносной полезной нагрузки в шаблон, который затем выполняется на стороне сервера [2].

Уязвимости SSTI могут поставить под угрозу веб-сайты, в зависимости от используемого механизма шаблонов и способа его использования в приложении. В некоторых случаях эти уязвимости могут не представлять реальной угрозы безопасности, но в большинстве случаев они могут иметь катастрофические последствия. Худший сценарий - злоумышленник может удаленно выполнить код и получить полный контроль над внутренним сервером для проведения других атак на внутреннюю инфраструктуру. Даже если удаленное выполнение кода невозможно, злоумышленники могут использовать уязвимости серверного шаблона в качестве основы для других атак и получить доступ к конфиденциальной информации и произвольным файлам на сервере [2].

Уязвимости внедрения шаблонов на стороне сервера возникают, когда пользовательский ввод объединяется в шаблоны, а не передается в виде данных. Для нахождения уязвимости SSTI злоумышленник может использовать строку вида *${{<%[%'"}}%* [2]. Если возникает исключение, это указывает на то, что внедренный синтаксис шаблона потенциально каким-то образом интерпретируется сервером. Это один из признаков того, что может существовать уязвимость к внедрению шаблонов на стороне сервера. Как и упоминалось выше эту уязвимость можно довести до других уязвимостей с более высокой критичностью. Допустим для чтения файла в шаблонизаторе Jinja, злоумышленник может использовать следующий

пейлоад : *{{ ''.__class__.__mro__[2].__subclasses__()[40]('/etc/passwd').read() }}*, а для выполнения кода : *{{ self.__init__.__globals__.__builtins__.__import__('os').popen('id').read() }}* [3].

Меры защиты [2]:

– лучший способ предотвратить внедрение шаблонов на стороне сервера - запретить пользователям изменять или отправлять новые шаблоны;

– использовать механизм шаблонов «без логики», такой как Mustache;

– выполнять пользовательский код только в изолированной среде, из которой потенциально опасные модули и функции полностью удалены;

– признать, что выполнение произвольного кода практически неизбежно, и применить собственную «песочницу», развернув среду шаблонов, например, в заблокированном контейнере Docker.

Заключение: SSTI (Server-side Template Injection) уязвимости являются серьезными угрозами безопасности, которые могут позволить злоумышленникам удаленно выполнять код и получать полный контроль над внутренним сервером. Для предотвращения этих уязвимостей следует применять различные меры: запускать пользовательский ввод в «песочнице», использовать шаблонизаторы «без логики» и т.п.

Библиографический список:

1. Что такое и зачем нужны шаблонизаторы HTML: [Электронный ресурс]. URL: https://habr.com/ru/companies/htmlacademy/articles/585956/. (Дата обращения: 16.02.2023)

2. Server-side template injection: [Электронный ресурс]. URL: https://portswigger.net/web-security/server-side-template-injection. (Дата обращения: 16.02.2023)

3. Server Side Template Injection: [Электронный ресурс]. URL: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server%20Side%20Template%20Injection/README.md. (Дата обращения: 16.02.2023)

УДК 004.056.53

Мисбахов Нияз Ильясович, студент
Лукьянов Эмиль Радикович, студент
Степанов Максим Олегович, студент

Ахметвалеев Амир Муратович, научный руководитель, кандидат технических наук, доцент кафедры «Систем информационной безопасности»

Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ
Россия, г. Казань

Misbakhov Niyaz Ilyasovich, student
Lukyanov Emil Radikovich, student
Stepanov Maxim Olegovich, student

Akhmetvaleev Amir Muratovich, scientific supervisor, candidate of technical sciences, associate professor of the department of "Information Security Systems"
Kazan National Research Technical University named after. A.N. Tupolev-KAI
Russia, Kazan

Обзор классификации OWASP Top 10

OWASP Top 10 classification overview

Аннотация: В статье выполняется обзор на OWASP Top 10 – список десяти основных угроз безопасности для веб-приложений, который служит руководством для программистов и специалистов по защите информации при разработке безопасных веб-решений. Рекомендации OWASP высоко ценятся аудиторами корпоративных систем. Данные рекомендации принято включать в жизненный цикл разработки программного обеспечения и использовать для формирования политик безопасности. В статье обсуждаются различные типы уязвимостей, приводятся их описания, причины возникновения, возможные последствия и стратегии по их предотвращению и смягчению. В статье также рассматриваются подходы к обеспечению безопасности веб-приложений на основе OWASP Top 10.
Ключевые слова: уязвимость, веб-приложение, OWASP, информационная безопасность, OWASP Top 10.
Annotation: This article reviews the OWASP Top 10, a list of the top ten security threats to web applications that serves as a guide for programmers and information security professionals in developing secure web solutions. OWASP recommendations are highly valued by auditors of corporate systems. These recommendations are usually included in the software development life cycle and used to formulate security policies. The article discusses various types of vulnerabilities, provides their descriptions, causes, possible consequences and strategies for their prevention and mitigation. The article also discusses approaches to securing web applications based on OWASP Top 10.
Key words: vulnerability, web application, OWASP, information security, OWASP Top 10.

OWASP (Open Web Application Security Project) - открытый проект по безопасности веб-приложений, созданный и поддерживаемый некоммерческой организацией OWASP Foundation. OWASP Top 10 представляет из себя обновляемый каждые 3 - 4 года список критических уязвимостей веб-приложений. Он помогает разработчикам и специалистам по информационной безопасности создавать и поддерживать безопасные сайты и приложения.

Разберем содержимое OWASP Top 10:

1) Нарушенный контроль доступа.

Контроль доступа обеспечивает соблюдение политики, согласно которой пользователи не могут действовать за пределами своих прав. Сбои обычно приводят к несанкционированному раскрытию информации, изменению или уничтожению всех данных или выполнению бизнес-функции за пределами возможностей пользователя [1].

2) Недостатки криптографии.

Недостатки криптографии представляют собой уязвимости, которые связаны с неправильной конфигурацией криптографической защиты. Они могут включать в себя недостаточную длину ключей, небезопасные условия их хранения, использование устаревших алгоритмов и прочие ошибки в реализации криптографии [2].

3) Инъекции.

Инъекция – это вредоносный ввод пользователя. Ввод, в большинстве своем представляет из себя вредоносные коды SQL, NoSQL, команд ОС, реляционного сопоставления объектов (ORM), LDAP и языка выражений (EL) или библиотеки навигации по графу объектов (OGNL).

Приложение уязвимо для атак такого рода при условии, что [1]:

– Данные, предоставленные пользователем, не проверяются, не фильтруются и не очищаются приложением;

– Динамические запросы или непараметризованные вызовы без контекстно-зависимого экранирования используются непосредственно в интерпретаторе;

– Вредоносные данные используются в параметрах поиска объектно-реляционного сопоставления (ORM) для извлечения дополнительных конфиденциальных записей;

– Вредоносный ввод напрямую объединяется с внутренними данными.

3) Небезопасная разработка архитектуры приложения.

Небезопасная разработка - это широкая категория, представляющая различные недостатки, выраженные отсутствием или неэффективной настройкой средств контроля. Одним из факторов, способствующих небезопасному проектированию, является отсутствие профилирования

бизнес-рисков, присущего разрабатываемому программному обеспечению или системе, и, следовательно, невозможностью определить, какой уровень безопасности требуется [1].

4) Неправильная конфигурация безопасности.

Небезопасная конфигурация - это ситуация, когда параметры приложения, сервера, базы данных или других системных компонентов не являются защищенными. Эта категория уязвимостей включает ненадежные или отсутствующие параметры аутентификации, авторизации и контроля доступа [2].

Например, если разработчик не ограничивает доступ к административной консоли приложения для пользователей без авторизации или с стандартными параметрами входа, злоумышленники могут легко получить доступ к этой панели и изменить ее настройки, фальсифицировать или украсть данные. Это распространенная ошибка, особенно среди начинающих разработчиков [2].

Приложение может быть уязвимым, при условии, что [1]:

– Отсутствуют соответствующие усиления безопасности в любой части стека приложений или неправильно настроенные разрешения для облачных служб;

– Включены или установлены ненужные функции (например, ненужные порты, службы, страницы, учетные записи или привилегии);

– Присутствуют учетные записи по умолчанию и их пароли по-прежнему включены и не изменяются;

– Обработка ошибок показывает пользователям трассировки стека или другие слишком информативные сообщения;

– В обновленных системах новейшие функции безопасности отключены или настроены небезопасно;

– Параметры безопасности на серверах приложений, платформах приложений (например, Struts, Spring, ASP.NET), библиотеках, базах данных и т. д. не имеют безопасных значений;

– Сервер не отправляет заголовки или директивы безопасности, или для них не установлены безопасные значения;

– Программное обеспечение устарело или уязвимо;

– Без согласованного и повторяемого процесса настройки безопасности приложений системы подвергаются более высокому риску;

6) Использование уязвимых или устаревших компонентов.

В эту группу уязвимостей относятся те случаи, когда приложение содержит компоненты, библиотеки, фреймворки, содержащие известные дефекты в безопасности. Для предотвращения этого, приложение должно периодически проверяться сканерами безопасности, так как ко многим

уязвимостям присутствуют открытые эксплоиты и ПО может стать легкой мишенью для злоумышленника.

7) Ошибки идентификации и аутентификации

Подтверждение личности пользователя, аутентификация и управление сеансами имеют решающее значение для защиты от атак, связанных с аутентификацией. В эту группу уязвимостей относятся слабые пароли, недостаточная проверка подлинности, неэффективные системы учёта сеансов и т.п.

8) Нарушения целостности программного обеспечения и данных.

Этот тип уязвимостей относятся к коду и инфраструктуре, которые не защищены от неправомерного изменения. Примером этого является ситуация, когда приложение использует плагины, библиотеки или модули из ненадежных источников, репозиториев и сетей доставки контента (CDN). Небезопасно настроенный процесс разработки может привести к несанкционированному доступу, вредоносному коду или компрометации системы. Также многие приложения теперь включают функцию автоматического обновления, при которой обновления загружаются без достаточной проверки целостности и применяются к ранее доверенному приложению. Злоумышленники потенциально могут загрузить свои собственные обновления для распространения и запуска на всех установках. Другим примером могут служить объекты или данные, закодированные или сериализованные в структуру уязвимой для небезопасной десериализации [1].

9) Ошибки ведения журнала и мониторинга безопасности.

Это уязвимости, при которых система некорректно регистрирует аномальные события, связанные с безопасностью. Они также включают отсутствие или неправильную конфигурацию механизмов журналирования и отсутствие оповещений о подозрительных событиях. Если в системе не осуществляется мониторинг безопасности, атаки злоумышленников могут оставаться незамеченными, что снижает вероятность быстрого реагирования на возникающие инциденты, обнаружения угроз и определения их источников. Предположим, что веб-приложение не ведет учет попыток неудачной аутентификации. Злоумышленник предпринимает многократные попытки взлома аккаунта пользователя или администратора, но разработчик этого не замечает, так как система не регистрирует эти действия [2].

10) Подделка запросов на стороне сервера.

Подделка запросов на стороне сервера (SSRF) - это уязвимость веб-безопасности, которая позволяет злоумышленнику заставить серверное приложение отправлять запросы в непредусмотренное место. При типичной атаке SSRF злоумышленник может заставить сервер подключиться к внутренним службам в инфраструктуре организации. В других случаях он может заставить сервер подключиться к произвольным внешним системам.

Это может привести к утечке конфиденциальных данных, таких как учетные данные авторизации [3].

Заключение: OWASP Top 10 является важным руководством для разработчиков и специалистов по безопасности при создании надежных и защищенных веб-приложений. Он представляет собой список из 10 наиболее опасных уязвимостей, которые могут быть использованы злоумышленниками для компрометации системы.

Для обеспечения безопасности веб-приложения, важно уделять внимание каждому из пунктов OWASP Top 10, начиная от неправильного проектирования и заканчивая недостатками в управлении привилегиями. Регулярное проведение аудита безопасности, использование современных инструментов и техник, а также обучение и повышение осведомленности команды разработчиков и администраторов помогут снизить риск возникновения уязвимостей и повысить общий уровень безопасности приложения.

Библиографический список:

1. OWASP Top Ten: [Электронный ресурс]. URL: https://owasp.org/www-project-top-ten/. (Дата обращения: 14.02.2024)

2. OWASP Top 10: самые распространённые уязвимости веб-приложений: [Электронный ресурс]. URL: https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyennye-uyazvimosti-vebprilozheniy/. (Дата обращения: 14.02.2024)

3. Server-side request forgery (SSRF): [Электронный ресурс]. URL: https://portswigger.net/web-security/ssrf. (Дата обращения: 17.02.2024)

УДК 004.056.53

Мисбахов Нияз Ильясович, студент
Степанов Максим Олегович, студент

Лукьянов Эмиль Радикович, студент
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ
Россия, г. Казань

Ахметвалеев Амир Муратович, научный руководитель, кандидат технических наук, доцент кафедры «Систем информационной безопасности»
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ
Россия, г. Казань

Misbakhov Niyaz Ilyasovich, student
Stepanov Maxim Olegovich, student
Lukyanov Emil Radikovich, student
Kazan National Research Technical University named after. A.N. Tupolev-KAI
Russia, Kazan

Akhmetvaleev Amir Muratovich, scientific supervisor, candidate of technical sciences, associate professor of the department of "Information Security Systems"
Kazan National Research Technical University named after. A.N. Tupolev-KAI
Russia, Kazan

Исследование методов эксплуатации уязвимости XXE

Research on exploitation methods for the XXE vulnerability

Аннотация: В данной статье анализируется уязвимость XXE в контексте безопасности систем, использующих формат XML. Рассмотрены причины возникновения XXE, потенциальные последствия эксплуатации уязвимости и основные ее разновидности. Для предотвращения XXE атак в статье рекомендованы конкретные методы, включая отключение поддержки внешних сущностей XML и проверку корректности обрабатываемых данных. Приводятся практические примеры XXE атак и рекомендации по противодействию им.
Ключевые слова: XXE, веб-приложение, уязвимость, XML, информационная безопасность.
Annotation: This article analyzes the XXE vulnerability in the context of the security of systems using the XML format. The causes of XXE, the potential consequences of exploiting the vulnerability and its main types are considered. To

prevent XXE attacks, the article recommends specific methods, including disabling support for external XML entities and checking the correctness of the processed data. Practical examples of XXE attacks and recommendations for countering them are provided.

Key words: XXE, web application, vulnerability, XML, information Security.

XXE (External XML Entity Injection) - это уязвимость в системе безопасности веб-приложений, которая позволяет хакерам вмешиваться в процесс обработки приложением данных в формате XML. Эта уязвимость часто позволяет хакерам получать доступ к файлам в файловой системе серверного приложения и взаимодействовать с другими серверными или сторонними системами, к которым приложение может иметь доступ [1].

Существуют различные типы атак XXE:

– Использование XXE для получения содержимого серверных файлов;
– Использование XXE для выполнения атак типа SSRF;
– Использование XXE для выполнения удаленных команд на сервере.

Стандарт XML предусматривает возможность использования DTD (document type definition). DTD даёт возможность определять и использовать XML-сущности. Сущности могут быть как полностью определены внутри документа (например, представлять собой какую-то строку), так и ссылаться на какой-то внешний ресурс. Отсюда и происходит название XXE-атаки: XML eXternal Entities [2].

Для реализации атаки XXE требуется [1]:

– Добавить DOCTYPE элемент, определяющий внешний объект;
– Изменить значения данных в XML, возвращаемом в ответе приложения, чтобы использовать определенный внешний объект.

Рассмотрим каждый тип XXE уязвимости. Предположим, что приложение для покупок проверяет существует ли пользователь с предоставленным именем, отправляя на сервер следующий XML-код:

```
<?xml version="1.0" encoding="UTF-8"?>
<userCheck><username>Bob</username></userCheck>
```

Злоумышленник может отправить запрос со следующим содержимым:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<userCheck><username>&xxe;</username></userCheck>
```

При отсутствии защиты от XXE сервер вернет содержание файла /etc/passwd, тем самым, злоумышленник может читать содержание файлов на сервере. Кроме схемы file, XML также поддерживает получение содержания из внешнего адреса, для этого можно воспользоваться следующим пейлоадом:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "http://internal.example.com/">
]>
```

<userCheck><username>&xxe;</username></userCheck>

Такая техника позволяет проводить атаки SSRF (подделка запросов на стороне сервера). Подделка запросов на стороне сервера - это уязвимость веб-безопасности, которая позволяет злоумышленнику заставить серверное приложение отправлять запросы в непредусмотренное место. При типичной атаке SSRF злоумышленник может заставить сервер подключиться к внутренним службам в инфраструктуре организации. В других случаях они могут заставить сервер подключиться к произвольным внешним системам. Это может привести к утечке конфиденциальных данных, таких как учетные данные авторизации [3].

В некоторых случаях атака XXE может привести к выполнению удаленного кода на сервере. Для этого требуется, чтобы программный поддерживал использование враппера expect. Пейлоад будет выглядеть следующим образом:

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [<!ENTITY xxe SYSTEM "expect://id">]>
<userCheck><username>&xxe;</username></userCheck>

Уязвимый сервер вернет вывод команды «id».

Практически все уязвимости XXE возникают из-за того, что библиотека синтаксического анализа XML приложения поддерживает потенциально опасные функции XML, которые приложению не нужны или которые они не собираются использовать. Самый простой и эффективный способ предотвратить атаки XXE - отключить эти функции [1].

Заключение: Уязвимость XXE является серьезной угрозой безопасности для систем, использующих XML. Она может привести к раскрытию конфиденциальной информации, нарушению работы приложений и выполнению удаленного кода. Предотвращение этой уязвимости включает в себя отключение потенциально опасных функций в синтаксическом анализаторе XML, обучение разработчиков об опасности использования этих функций и применение соответствующих инструментов для обнаружения XXE-атак.

Библиографический список:

1. XML external entity (XXE) injection: [Электронный ресурс]. URL: https://portswigger.net/web-security/xxe. (Дата обращения: 16.02.2024)
2. XXE-атака (XML External Entity): [Электронный ресурс]. URL: https://pvs-studio.ru/ru/blog/terms/6546/. (Дата обращения: 16.02.2024)
3. Server-side request forgery (SSRF): [Электронный ресурс]. URL: https://portswigger.net/web-security/ssrf. (Дата обращения: 16.02.2024)

УДК 004.8

Николаев Владислав Антонович,
обучающийся кафедры систем информационной безопасности
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ»
Россия, г. Казань

Гуляев Иван Андреевич,
обучающийся кафедры систем информационной безопасности
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ»
Россия, г. Казань

Nikolaev Vladislav Antonovich,
student of the Department of Information Security Systems
Federal State Budgetary Educational Institution of Higher Education "Kazan National Research Technical University named after. A.N. Tupolev-KAI"
Russia, Kazan
Gulyaev Ivan Andreevich,
student of the Department of Information Security Systems
Federal State Budgetary Educational Institution of Higher Education "Kazan National Research Technical University named after. A.N. Tupolev-KAI"
Russia, Kazan

Новый этап в развитии квантовых технологий: квантовая связь через взаимодействие между атомами

A new stage in the development of quantum technologies: quantum entanglement through interactions between atoms

Аннотация: В данной работе решается задача лучшего понимания свойств материалов на атомном уровне. Для решения данной задачи было взято исследование из Вашингтонского университета. Ученые обнаружили, что они могут «услышать» атомное взаимодействие, другими словами, механические колебания между слоями атомов, наблюдая за тем, как свет, излучаемый этими атомами, меняется при воздействии на них лазером. Напомним, что атомное взаимодействие – это сила, которая связывает атомы в молекуле или кристалле. Она возникает из-за того, что электроны в атомах могут занимать только определенные энергетические уровни, и переход между этими уровнями происходит с выделением или поглощением энергии. Данные «звуки» атомного взаимодействия могут помочь исследователям создавать и передавать квантовые данные. Стоит отметить, что этот звук, известный как звук атомного взаимодействия, может быть использован для

создания новых методов передачи и обработки квантовой информации. Например, исследователи могут использовать этот звук для создания более эффективных квантовых компьютеров и систем связи. Это может привести к новым открытиям в области квантовых технологий. Данное открытие способствует созданию новых материалов с улучшенными свойствами, которые могут быть использованы в квантовых компьютерах и системах связи. Также исследование атомного взаимодействия может помочь в разработке новых методов защиты квантовой информации от ошибок, что является одной из главных проблем в развитии квантовых технологий сегодня.

Abstract: This paper addresses the challenge of better understanding the properties of materials at the atomic level. To solve this problem, a study from the University of Washington was taken. Scientists found that they can "hear" the atomic interaction, in other words, mechanical vibrations between layers of atoms, by observing how the light emitted by these atoms changes when they are exposed to a laser. Recall that atomic interaction is the force that binds atoms together in a molecule or crystal. It arises because electrons in atoms can occupy only certain energy levels, and the transition between these levels occurs with the release or absorption of energy. These "sounds" of atomic interaction can help researchers create and transmit quantum data. It is worth noting that this sound, known as the sound of atomic interaction, can be used to create new methods for transmitting and processing quantum information. For example, researchers can use this sound to create more efficient quantum computers and communication systems. This could lead to new discoveries in quantum technology. This discovery contributes to the creation of new materials with improved properties that can be used in quantum computers and communication systems. Also, the study of atomic interaction can help in developing new methods of protecting quantum information from errors, which is one of the main problems in the development of quantum technologies today.

Ключевые слова: атомное взаимодействие, механические колебания, квантовая информация, квантовые компьютеры, лазерное воздействие, звуковые волны, передача данных, квантовые технологии, новые материалы, ошибки в данных, защита информации.

Key words: atomic interaction, mechanical vibrations, quantum information, quantum computers, laser impact, sound waves, data transmission, quantum technologies, new materials, data errors, information protection.

1. Введение

В последние годы наблюдается значительный рост интереса к квантовым технологиям, в частности, к квантовым вычислениям. Это связано с тем, что квантовые компьютеры обладают значительно большей вычислительной мощностью по сравнению с классическими компьютерами. Одним из

ключевых аспектов квантовых вычислений является передача и хранение квантовой информации. Кроме того, из-за большого числа задач, решаемых в данных системах, их многокритериальности и нечеткого характера возникает необходимость поиска эффективного подхода в решении данных задач. В данной статье мы представляем результаты исследования, посвященного изучению возможности использования атомных колебаний для отслеживания и передачи квантовой информации.

Специалисты из Вашингтонского университета выявили возможность отслеживания атомных вибраций, или механических колебаний между двумя рядами атомов, с помощью лазера, который заставляет атомы испускать свет. Этот процесс можно использовать для записи и передачи квантовой информации.

Разработанное устройство может стать основой для новых коммуникационных систем, высокоточных сенсоров и мощных вычислительных систем. Это открытие может привести к революции в области квантовых технологий, обеспечивая более быструю и точную обработку данных, а также безопасные и надежные системы связи.

Результаты исследования были опубликованы 1 июня 2023 года в университете «University of Washington» [1].

2. Описание и особенности предметной предметной области

«Это новая атомно-масштабная платформа, основанная на том, что научное сообщество именует «оптомеханикой». В ней свет и механические колебания неразрывно связаны между собой», – рассказывает старший профессор по электротехнике, вычислительной технике и физике. «Это обеспечивает новый тип задействованного квантового явления, которое может использоваться для контроля одиночных фотонов, проходящих через интегрированные оптические цепи, для множества применений».

Ранее команда изучала квазичастицу квантового масштаба, известную как «экситон». Рассмотрим систему квазичастиц, которые могут выступать электронами, фононами, магнонами и другими. Экситон и фотон являются двумя разными типами частиц. Экситон обладает определенной энергией и импульсом и может перемещаться по кристаллу. Фотон, с другой стороны, является частицей света. Он также обладает энергией и импульсом, но в отличие от экситона, он не имеет массы и может двигаться со скоростью света. Экситоны играют важную роль в процессах поглощения и излучения света в полупроводниках, а фотоны используются для передачи информации на большие расстояния. Каждая квазичастица имеет свою энергию, импульс и массу. Квазичастицы могут взаимодействовать друг с другом, и их взаимодействие описывается законами квантовой механики [2,3]. Можно заложить информацию в экситон и затем извлечь ее в виде фотона – мельчайшей частицы энергии, которая считается квантом света. Свойства фотона, такие как поляризация, длина волны и время испускания, могут

использоваться как квантовый бит информации, или «кубит», для квантовых вычислительных и коммуникационных процессов. В связи с тем, что этот «кубит» переносится фотоном, последний перемещается со скоростью света.

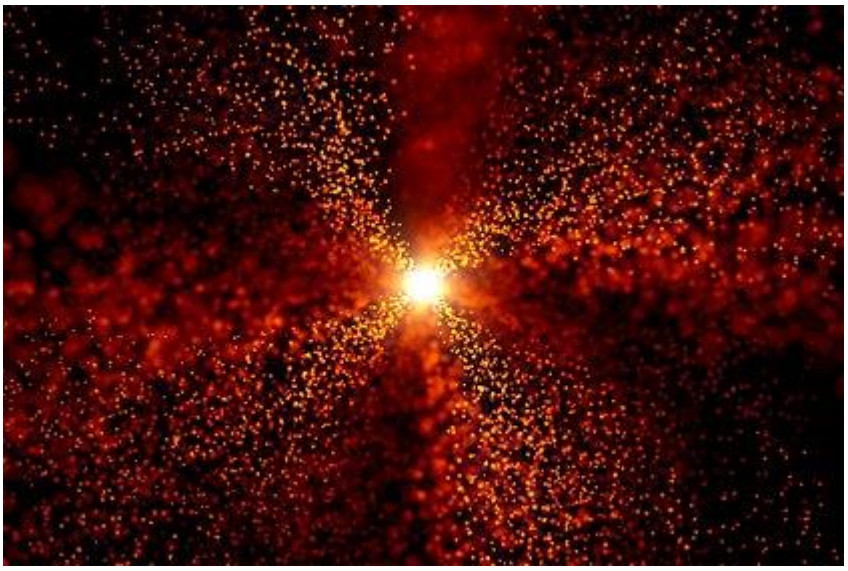


Рисунок 1 – Визуальное представление кванта света

«С точки зрения более широкой перспективы, это исследование подчеркивает, что для построения квантовой сети мы должны иметь методы надежного создания, обработки, хранения и передачи квантовых битов информации (кубитов). Фотоны – самый подходящий кандидат для переноса квантовой информации на большие расстояния, поскольку оптические волокна позволяют передавать фотоны с высокой скоростью с минимальными потерями энергии или информации», – говорит главный автор исследования.

Исследователи работали с экситонами для создания однофотонного излучателя, или «квантового эмиттера», который является важным компонентом для квантовых технологий [4,5], связанных со светом и оптикой. Для этого они поместили два тонких слоя вольфрамовых и селеновых атомов, известных как диселенид вольфрама, один поверх другого.

Когда исследователи использовали определенный импульс лазерного излучения, они выбивали электрон из атома диселенида вольфрама, создавая экситон. Каждый экситон представляет собой комбинацию отрицательно заряженного электрона в одном слое материала и положительно заряженной «дырки» в другом слое, где отсутствующий электрон был. Из-за взаимного притяжения зарядов, электрон и «дырка» в каждом экситоне плотно связаны. Через некоторое время, когда электрон опускается обратно в «дырку», которую он изначально занимал, экситон высвобождает один фотон,

несущий квантовую информацию – создавая квантовый источник света, к которому стремилась команда.

Но команда обнаружила, что атомы диселенида вольфрама излучают другой тип квазичастиц, так называемые фононы. Эти фононы являются результатом вибрации атома, похожей на дыхание. В этом случае два слоя атомов диселенида вольфрама действуют как крошечные мембраны, вибрируя друг относительно друга и создавая фононы. Это первый раз, когда такие фононы были замечены в одном фотонном источнике в двумерной атомной системе этого типа.

3. Проблемы и решения

Когда ученые измерили спектр излучения света, они обнаружили несколько одинаковых пиков. Каждый фонон, испущенный экситоном, связан с одним или несколькими другими фононами, что аналогично подъему по энергетической шкале квантов на одну ступеньку за раз. На спектре эти скачки энергии представлены в виде равноудаленных пиков.

Безопасность и защита данных также представляют значительный вызов в распределенной и мультиоблачной среде [6,7], поскольку необходимо защищать систему от внешних угроз и внутренних уязвимостей. Кроме того, поддержание высокого уровня производительности при масштабировании системы, особенно в глобальных приложениях с большими объемами данных, является сложной задачей.

Фонон – квазичастица, квант энергии согласованного колебательного движения атомов твёрдого тела, образующих идеальную кристаллическую решётку.

Модельное представление колебаний решётки как совокупности фононов оказывается удобным при анализе взаимодействия электронов, световых квантов и других частиц, доля импульса которых может быть передана решётке.

Согласно концепции корпускулярно-волнового дуализма, любой объект может восприниматься и как волна, и как частица (квазичастица). Например, свет может трактоваться как совокупность электромагнитных волн или как поток фотонов, движущихся (в случае вакуума) со скоростью.

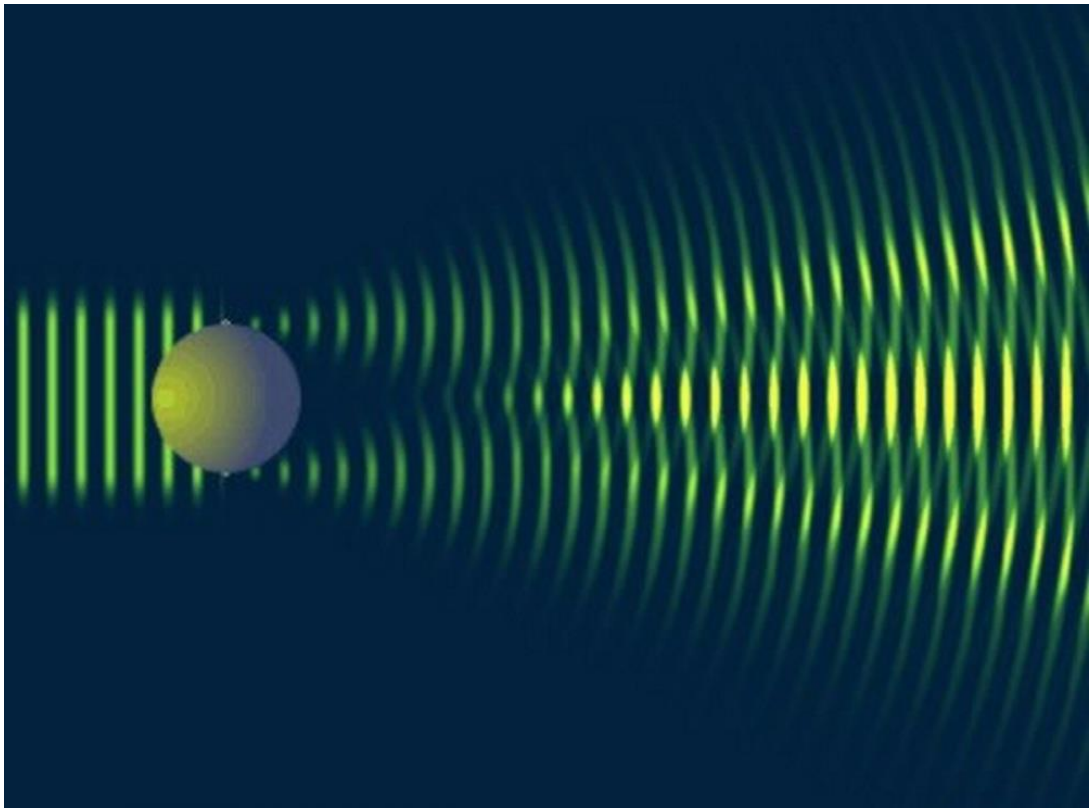


Рисунок 2 – Совокупность электромагнитных волн

Амплитуда волн и плотность потока соответствуют друг другу таким образом, чтобы обеспечилась одинаковость спектральной плотности мощности в обеих трактовках [8,9]. В квантовой механике, концепция дуализма используется для элементарных частиц, включая электроны.

Аналогичным образом упругие волны (в узком смысле слова – звук) могут восприниматься как поток квазичастиц, носящих название фононов. Соответственно, состояние кристаллической решётки может рассматриваться как газ фононных квазичастиц (подобно более привычным электронному или фотонному газам).

Ученые заинтересовались возможностью использования фононов в квантовых технологиях. Приложив электрическое напряжение, они обнаружили, что можно изменять энергию взаимодействия между связанными фононами и испускаемыми фотонами. Они смогли измерить и проконтролировать эти изменения.

4. Заключение

С помощью разработанного комплекса коллектив исследователей, упомянутых выше, ставит задачу создания системы с квантовыми источниками, которые помогут в укоренном и качественном режиме проводить квантовые расчеты и квантовую диагностику [10,11].

Далее коллектив намерен разработать оптический волновод – интегрально-оптическое устройство, способное принять фотон и направить его в требуемом направлении. Затем предполагается масштабировать эту систему.

Вместо возможности контроля над одним источником квантовых частиц команда стремится к управлению несколькими источниками и связанными с ними колебательными состояниями. Таким образом, квантовые источники смогут сообщаться друг с другом, формируя основу для квантовых сетей [12].

Основная цель коллектива [1] – создание комплексной системы с квантовыми источниками, способной использовать отдельные фотоны, движущиеся по оптическим каналам, и недавно обнаруженные фононы в целях квантовых расчетов и квантовой диагностики. Как говорит один из ученых, это достижение, без сомнения, внесет вклад в данную работу и окажет поддержку в дальнейшем прогрессе квантовых вычислений с множеством потенциальных применений в будущем.

Библиографический список:

1. Университет Вашингтона. Новый строительный блок для квантовой технологии [Электронный ресурс]. Режим доступа: https://www.ece.uw.edu/. (Дата обращения: 12.12.2023).
2. Свидетельство о государственной регистрации программы для ЭВМ № 2021613638 Российская Федерация. Программа ассоциативной защиты файлов "Stego" : № 2021612051 : заявл. 20.02.2021 : опубл. 11.03.2021 / И. С. Вершинин, Р. Ф. Гибадуллин ; заявитель федеральное государственное бюджетное образовательное учреждение высшего образования "Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ".
3. Гибадуллин, Р. Ф. Система баз данных картографии с ассоциативной защитой : специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность" : автореферат диссертации на соискание ученой степени кандидата технических наук / Гибадуллин Руслан Фаршатович. – Уфа, 2011. – 16 с.
4. Гибадуллин, Р. Ф. Параллельный модуль исполнения пространственных запросов к защищенной картографической базе данных / Р. Ф. Гибадуллин, А. А. Новиков // Поиск эффективных решений в процессе создания и реализации научных разработок в российской авиационной и ракетно-космической промышленности : Международная научно-практическая конференция, Казань, 05–08 августа 2014 года. Том II. – Казань: Издательство Казанского государственного технического университета, 2014. – С. 422-424.
5. Двумерно-ассоциативная защита информации в картографических системах / В. А. Райхлин, И. С. Вершинин, Р. Ф. Гибадуллин, С. В. Пыстогов // Проблемы и перспективы развития наукоемкого машиностроения : Международная научно-техническая конференция, Казань, 19–21 ноября

2013 года. – Казань: Казанский государственный университет, 2013. – С. 48-50.
6. Гибадуллин, Р. Ф. Применение графических ускорителей при обработке SQL-запросов / Р. Ф. Гибадуллин, А. Г. Савельев, А. А. Новиков // Новые технологии, материалы и оборудование российской авиакосмической отрасли - акто-2016 : сборник докладов Всероссийской научно-практической конференции с международным участием: в 2-х томах, Казань, 10–12 августа 2016 года. Том 2. – Казань: Академия наук Р, 2016. – С. 56-62.
7. Гибадуллин, Р. Ф. Защищенное управление беспроводной передачей картографической информации / Р. Ф. Гибадуллин, И. М. Гапдулхаков // Наука в движении: от отражения к созданию реальности : Материалы Всероссийской научно-практической конференции [Электронное издание], Альметьевск, 15 июня 2016 года / Под общей редакцией М.Ш. Гарифуллиной. – Альметьевск: Издательство "Перо", 2016. – С. 236-238.
8. Свидетельство о государственной регистрации программы для ЭВМ № 2016611421 Российская Федерация. Программа управления ассоциативно защищенными картографическими базами данных "Security Map Cluster" : № 2015662153 : заявл. 10.12.2015 : опубл. 02.02.2016 / И. С. Вершинин, Р. Ф. Гибадуллин, С. В. Пыстогов ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ» (КНИТУ-КАИ).
9. Ямалеева, Г. Н. Оптимизация исполнения SQL-запросов к базам данных под управлением MySQL / Г. Н. Ямалеева, М. Ю. Перухин, Р. Ф. Гибадуллин // Информационные технологии и математическое моделирование (ИТММ-2017) : Материалы XVI Международной конференции имени А.Ф. Терпугова, Казань, 29 сентября – 03 2017 года. Том Часть 2. – Казань: Издательство научно-технической литературы, 2017. – С. 239-241.
10. Гибадуллин, Р. Ф. Исследование производительности технологий OpenMP и OpenCL / Р. Ф. Гибадуллин, Р. Ш. Минязев, А. А. Баев // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. – 2018. – № 2(38). – С. 43-50. – DOI 10.15350/2306-2819.2018.2.43.
11. Белашова, Е. С. Сети и системы передачи информации : учебное пособие / Е. С. Белашова, Р. Ф. Гибадуллин, А. Р. Мухутдинов. – Казань : РИЦ "Школа", 2021. – 100 с.
12. Гибадуллин, Р. Ф. Ассоциативная защита числовых сведений в текстовых документах с применением библиотеки Parallel Framework платформы .NET / Р. Ф. Гибадуллин, И. С. Вершинин // Computational Nanotechnology. – 2023. – Т. 10, № 3. – С. 121-129.

DOI 10.34755/IROK.2024.12.84.021
УДК 004.9

Портнов Константин Валерьянович,
к.т.н., доцент кафедры прикладная информатика, ФГАОУ ВО
«Самарский государственный экономический университет»
Россия, г.Самара

Портнова Наталья Юрьевна
Преподаватель, Лингвистический центр «Английский»
Россия, г.Самара

Сибарцева Елизавета Валерьевна
Обучающийся, Лингвистический центр «Английский»
Россия, г.Самара

Portnov Konstantin Valeryanovich,
Candidate of Technical Sciences, Associate Professor of the Department of Applied Informatics, Samara State Economic University
Russia, Samara

Portnova Natalya Yurievna
Teacher, Linguistic Center "English"
Russia, Samara

Sibartseva Elizaveta Valerievna
Student, Linguistic Center "English"
Russia, Samara

Автоматизированные информационные системы анализа и обработки данных в медицине

Automated information systems for data analysis and processing in medicine

Аннотация: В работе представлены результаты разработки информационной системы обработки медицинских данных, на базе данных полученных в результате экспорта из медицинских информационных систем.

Автоматизированная информационная система реализовывалась на основе корреляционного анализа.
Ключевые слова: автоматизация, бизнес-процесс, медицинские учреждения, медицинская информационная система.
Annotation: The paper presents the results of the development of an information system for processing medical data, based on data obtained as a result of export from medical information systems. The automated information system was implemented based on correlation analysis.
Key words: automation, business process, medical institutions, medical information system

Автоматизация бизнес-процессов набрала большую популярность на современном рынке. Это оправдывается тем, что механизмы автоматизации позволяют значительно сократить издержки любого производства, а значит – повысить эффективность деятельности предприятия.

Бизнес-процесс – это совокупность взаимосвязанных и взаимодействующих видов деятельности, в рамках которой «на входе» используется один или более видов ресурсов, и в результате этой деятельности «на выходе» создается продукт, представляющий ценность для потребителя.

Целью автоматизации бизнес-процессов, в том числе и медицинской деятельности, является попытка скоординировать работу организации, обеспечить более быстрые способы обработки данных и устранить влияние человеческого фактора на деятельность в целом. Медицину трудно представить без автоматизированных информационных систем, как внедренных в устройства управления технических приборов, так и в процессах документооборота.

Основные задачи в области дигитализации медицинских процессов отмечаются: консультативные услуги для медицинского персонала и пациентов, системы электронных медкарт (историй болезни), цифровизация медицинского страхования, аптечной информации включая обеспечение информацией потенциальных покупателей, заказа мед. оборудования и материалов, диспетчерские системы скорой помощи.

Рассмотрев большое количество материалов, и проанализировав их, мы можем выявить проблемы предметной области, на основании рассмотренных проблем мы можем выделить следующие проблемы:

1. Государственное регулирование отрасли, а также создание государственных глобальных систем в области здравоохранения.
2. Долгосрочность разработки МИС и затяжной этап ее внедрения и отладки

3. При внедрении медицинских информационных систем является отсутствие участия и желания врачей к переходу к новому формату функционирования.

4. Существуют определенные правила и стандарты для МИС, установленные законодательством, которые невозможно игнорировать, это может вызвать серьезные проблемы и последствия.

5. Положение о медицинский информационной системе в медицинской организации может обязывать использовать АИС, которая входит в состав единой региональной, федеральной или государственной информационной структуры, либо соответствует определенным стандартам и понятиям.

6. В современной реальности существуют и продалжают создаваться ряд программных и аппаратных решений в области электронной медицины и здравоохранения, в этой области работают ряд крупных фирм, иностранного и отечественного происхождения 1С, Cisco, AGFA, GE и другие

7. Проблемы связи в регионах, т.к. системы современной медицины напрямую связано с наличием на местах скоростных каналов связи

Цели анализа и обработки данных в медицинских учреждениях могут иметь несколько направлений:

- Выявление зависимости
- прогнозирование,
- классификация клинических случаев (диагностика),
- поиск похожих клинических случаев,
- наблюдение за состоянием пациентов.
- сегментирование рынка
- принятие управленческих решений

Статистический анализ ставит задачу найти связь, ассоциацию, зависимость между исходом и факторами, предположительно влияющими на исход, доказать, что они связаны в статистическом смысле, если возможно, оценить степень этой связи.

При разработке АИС анализа медицинских данных мы будем использовать корреляционный анализ. Корреляционный анализ при анализе данных полученных из историй болезни и определяет коэффициенты корреляции, на основании которых могут быть получены данные насколько согласованно изменение одних величин относительно других, в частности зависимости между анализами ТТГ Т3 и Т4 изменения которых коррелирует между собой.

Формулирование основной гипотезы исследования включает формулирование нулевой гипотезы (H_0) являющейся отправной точкой исследования, и перехода к следующей гипотезе(H_i) до получения научно значимых результатов. Нулевая гипотеза является «основным состоянием»,

которое, является своего рода «аксиоматической» точкой, которая верна в отсутствии убедительных доказательств, и альтернативной гипотезы (H_A) , которая будет принята после соответствующих доказательств. Проще говоря, нулевая гипотеза будет сохраняться до тех пор пока не будет доказательств обратного.

В качестве оценивания ошибок используется оценка степени отклонения между характеристиками выборки и популяции. Различают два вида ошибок: случайную ошибку и систематическую ошибку, возникающую вследствие нарушения правил отбора (или из-за смешений при отборе).

В медико-биологических исследованиях, проверка гипотезы существенно важна, т.к. она позволяет исследователям обобщить выводы о значимых процессах, которые базируются на исследовательской выборке, на всю популяцию.

Целью проверки гипотез является определение статистической значимости. Проверка гипотезы может подтвердить или отклонить утверждение о том. что наблюдаемые результаты не случайны. а отражают связь между переменным.

Коэффициент корреляции Пирсона рассчитывается по формуле 4

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\bar{y})^2}} \quad (4)$$

где,

n - размер выборки

x_i,y_i –значения наблюдаемых величин

После накопления данных, как правило, в какой-либо из распространенных СУБД – MS SQL Server возникает задача их обработки, с ранее описанными целями. Однако перед обработкой необходимо произвести экспорт из хранилища в удобной форме. В случае если МИС система собственной разработки, то трудностей не возникает. В случае же использовании сторонней МИС возникает необходимость разработки интерфейса для экспорта данных в удобной форме пригодной для их последующей обработки.

В частности в случае установления зависимости между тяжестью поражения легочной ткани и наличием витаминов группы «D» в случае лечение заболевания вирусной пневмонии вызванной вирусом Эпштейн-Барр, необходимо экспортировать из историй болезни данные об анализах на витамины группы «D», а также результаты КТ легких. Подобные данные являются по сути записями соответствующих таблиц.

Возникает необходимость в изучении архитектура базы данных и пониманию мест хранилища тех или иных данных. Таким образом, в ходе анализа необходимо провести анализ архитектуры базы данных медицинской

информационной системы и сформировать ERD-диаграмму отражающую строение базы данных или ее фрагмента. После понимание архитектура базы данных, наличия аутентификационных данных, предустановленной СУБД, формирование данных можно произвести путем соответствующего SQL-запроса.

Блок-схема архитектуры системы анализа и обработки данных представлена на рисунке 1.

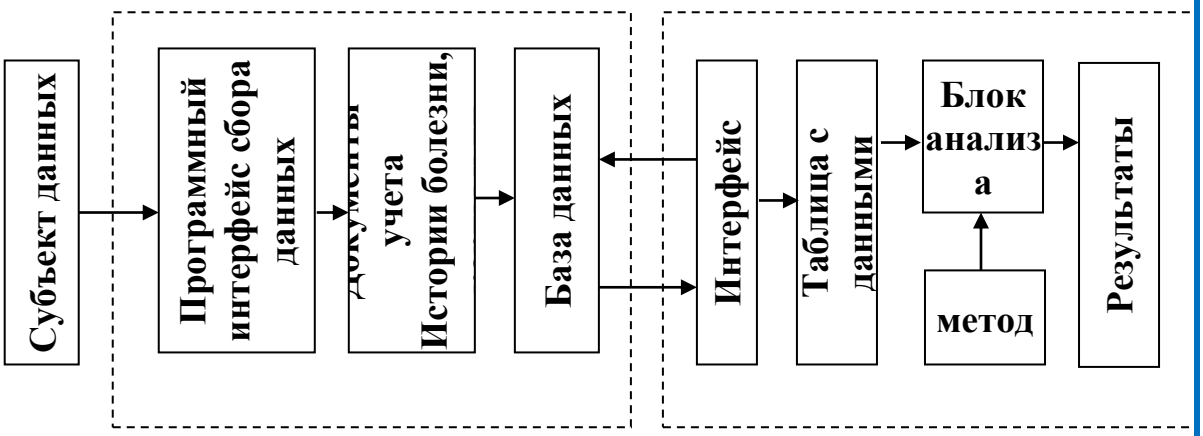


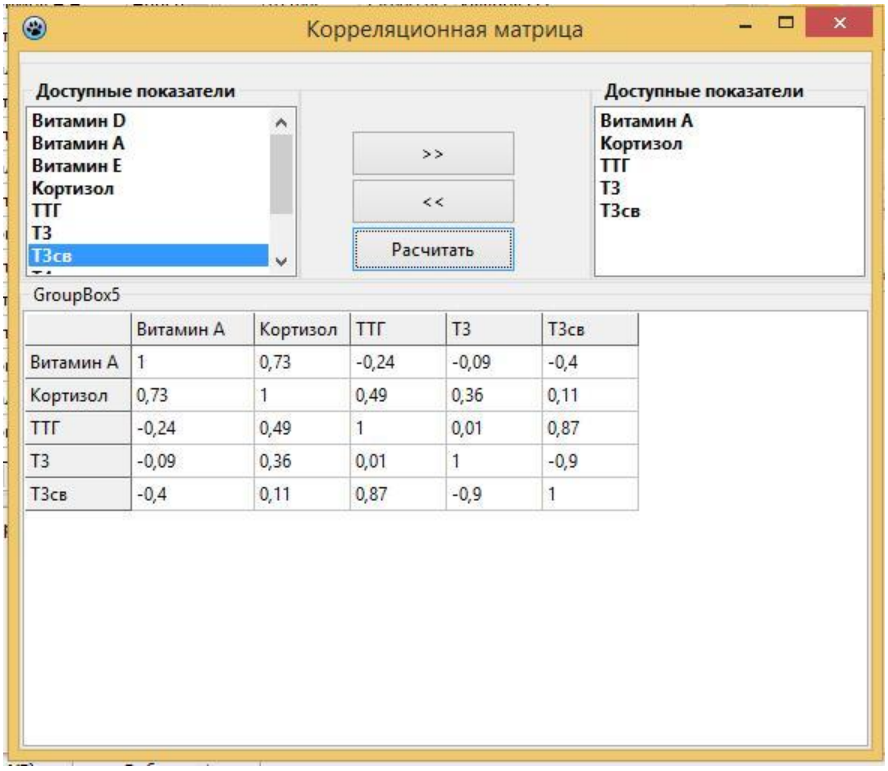
Рисунок 1 - Архитектуры системы анализа и обработки данных

При разработке системы анализа данных нами реализовывался блок анализа с использованием корреляционного анализа между тяжестью болезни и наличием определенных медицинских признаков.

Корреляционный анализ способствует установлению зависимости между двумя этими показателями, а также характеристиками этой связи - форму связи, направление и силу связи.

Статистический анализ является интегральной частью клинического исследования. Проектируемая система призвана помочь клиницистам разобраться в сути и принципах применения различных методов обработки медицинских данных, не углубляясь в детали математических расчетов. В обзоре рассмотрены наиболее востребованные и популярные статистические методы анализа данных, применяемые в клинической и экспериментальной медицине.

В результате в пробной версии системы нами был построен график зависимости и рассчитан коэффициент Пирсона равен -0,7795 что говорит высокая отрицательной связи.



	Витамин А	Кортизол	ТТГ	Т3	Т3св
Витамин А	1	0,73	-0,24	-0,09	-0,4
Кортизол	0,73	1	0,49	0,36	0,11
ТТГ	-0,24	0,49	1	0,01	0,87
Т3	-0,09	0,36	0,01	1	-0,9
Т3св	-0,4	0,11	0,87	-0,9	1

Рисунок 2 – Главное окно модуля по анализу данных

В перспективе планируется дополнить систему такими показателями как:

- Коэффициент ранговой корреляции Спирмена
- Коэффициент ранговой корреляции Кендалла
- Коэффициент ранговой корреляции Гудмена - Краскела

Таким образом результатами данной работы являются:

1. Анализ источников получения данных
2. Анализ фрагментов структура базы данных
3. Создание интерфейса для сбора данных через СУБД
4. Алгоритм обработки данных для получения коэффициента Пирсона
5. Графическое распределение изучаемой выборки

Библиографический список:

1. Сахбиева А.И., Калякина И.М., Косников С.Н., Латушкина Т.С., Майорова И.А. Цифровизация экономика и обеспечение безопасности данных // Московский экономический журнал. 2021. № 8. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-8-2021-28/ Иноземцев, В. Л. На рубеже эпох. Экономические тенденции и их неэкономические следствия [Текст] / В.Л. Иноземцев. - М. : Экономика, 2003. – 730 с.

2. Портнов, К. В. Генетические алгоритмы и поиск эффективных порядков индикаторов в биржевой торговой стратегии на основе пересечения трех скользящих средних / К. В. Портнов // Вестник Самарского государственного технического университета. Серия: Технические науки. – 2005. – № 32. – С. 72-76. – EDN JWUXKZ.

3. Евсеева А.К., Пожарнова А.А., Портнов К.В. Облачные технологии, вопросы безопасности // В сборнике: Тренды развития современного общества: управленческие, правовые, экономические и социальные аспекты. Сборник научных статей 11-й Всероссийской научно-практической конференции. Курск, 2021. С. 71-73.

4. Латушкина Т.С., Майорова И.А.,Яковлев, Использование и применение javascript-фреймворков (react, angular, vue.js) для разработки web-приложений/Экономика и предпринимательство. 2023. № 9 (158). С. 1374-1376

5. Портнов, К. В. Модификация модели генетических алгоритмов с применением нечеткого оператора выбора точки Кроссовера / К. В. Портнов // Математическое моделирование и краевые задачи : Труды Второй Всероссийской научной конференции, Самара, 01–03 июня 2005 года / Редколлегия: В. П. Радченко (отв. редактор), Э. Я. Рапопорт, Е. Н. Огородников, М. Н. Саушкин (отв. секретарь). Том Часть 2. – Самара: Самарский государственный технический университет, 2005. – С. 203-205. – EDN TGCFVB.

УДК 004.056

Степанов Максим Олегович, студент
Лукьянов Эмиль Радикович, студент
Мисбахов Нияз Ильясович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Нагаев Назим Харисович, научный руководитель, старший преподаватель кафедры «Системы информационной безопасности»
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, student
Lukyanov Emil Radikovich, student
Misbachov Niaz Ilyasovich, student
Kazan National Israeli Technical University named A.N. Tupolev-KAI
Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer of the Department of "Information security system"
Kazan National Israeli Technical University named A.N. Tupolev-KAI
Russia, Kazan

Биометрическая аутентификация: методы, преимущества и недостатки

Biometric authentication: methods, advantages and disadvantages

Аннотация: В данной статье рассматриваются значимость и перспективы использования биометрической аутентификации в обеспечении безопасности и защите данных в различных областях. Описываются основные методы биометрической аутентификации, их преимущества по сравнению с традиционными методами и проблемы. Отмечается значимость развития и совершенствования биометрических технологий для обеспечения более эффективной защиты информации.
Ключевые слова: биометрическая аутентификация, методы, информационная безопасность, защита данных.
Abstract: This article discusses the importance and prospects of using biometric authentication in ensuring data security and protection in various fields. The main methods of biometric authentication, their advantages over traditional methods and problems are considered. The importance of the development and improvement of biometric technologies to ensure more effective information protection is noted.
Keywords: biometric authentication, methods, information security, data protection.

В наше время, когда цифровые технологии становятся все более распространенными и играют все более важную роль во всех сферах жизни,

вопрос обеспечения информационной безопасности и аутентификации становится критически важным. Тенденции последних лет показываю, что традиционные, ставшие привычными для нас, методы аутентификации, такие как пароли, пин-коды, токены и карты, все чаще подвергаются различного типа кибератакам со стороны хакеров и злоумышленников. В этой связи, биометрическая аутентификация становится все более актуальной и перспективной технологией.

Биометрическая аутентификация — это процедура проверки по уникальным физическим и поведенческим характеристикам для подтверждения личности человека, который обращается с целью получения услуги или доступа к конфиденциальной информации [1]. Вместо использования паролей, пин-кодов или токенов, биометрическая аутентификация использует информацию, которая является неотъемлемой частью человека, чтобы подтвердить его или ее идентичность.

Физиологические характеристики, используемые в биометрической аутентификации, включают отпечатки пальцев, структуру лица, радужную оболочку глаза, голос и генетические данные, такие как ДНК. Поведенческие характеристики включают подпись, походку или способ набора текста на клавиатуре.

Различные методы биометрической аутентификации используют разные физиологические или поведенческие характеристики человека для проверки его личности. Рассмотрим наиболее распространенные методы [2,3]:

– Распознавание лиц: Метод распознавания лиц анализирует уникальные черты лица, такие как форма, размер и расположение глаз, носа и рта. Система захватывает изображение лица и сравнивает его с сохраненными шаблонами лиц в базе данных. Распознавание лиц широко применяется в системах видеонаблюдения, мобильных устройствах и системах контроля доступа.

– Распознавание отпечатков пальцев: Метод распознавания отпечатков пальцев основан на уникальных узорах, которые присутствуют на поверхности пальцев каждого человека. Распознавание отпечатков пальцев широко применяется в системах контроля доступа, таких как здания, компьютеры и сейфы, а также в мобильных устройствах, чтобы обеспечить безопасность и удобство использования. Оно также используется в паспортах и других документах для подтверждения личности.

– Распознавание радужной оболочки: Метод распознавания радужной оболочки анализирует уникальные узоры в радужной оболочке глаза. При помощи этого метода система захватывает изображение глаза и проводит сопоставление полученных данных с предварительно сохраненными шаблонами. Распознавание радужной оболочки обычно используется в специализированных системах безопасности.

– Распознавание голоса: Метод распознавания голоса анализирует уникальные характеристики голоса, такие как высота, тембр, интонация и речевые особенности. Система анализирует голосовой образец, извлекает его характеристики и сравнивает их с предварительно сохраненными шаблонами в базе данных. Распознавание голоса используется в системах голосового управления, банковских услугах и телефонных системах автоматического определения личности.

– Распознавание почерка: Метод распознавания почерка анализирует уникальные характеристики почерка человека, такие как форма букв, наклон, размер и давление пера на бумагу. Система записывает написанный текст и сравнивает его с сохраненными шаблонами в базе данных. Распознавание почерка может использоваться в системах банковского обслуживания и юридических документах.

Каждый из этих методов имеет свои преимущества и недостатки. Некоторые методы, такие как распознавание лиц и отпечатков пальцев, обладают высокой точностью и широко применяются в различных областях. Другие методы, такие как распознавание радужной оболочки, голоса и почерка, могут быть менее распространены, но обеспечивают дополнительные уровни безопасности и уникальности. Выбор метода биометрической аутентификации зависит от конкретных требований системы и предпочтений пользователей.

Биометрическая аутентификация предлагает ряд преимуществ по сравнению с традиционными методами аутентификации, такими как пароли или токены.

Одним из основных преимуществ биометрической аутентификации является ее удобство. Биометрические данные, такие как отпечатки пальцев или лицо, всегда доступны у пользователя и не требуют запоминания или переноски дополнительных устройств или информации. Например, вместо ввода пароля или вставки токена, пользователю достаточно просто предъявить свое лицо или отпечаток пальца для подтверждения своей личности. Это сокращает необходимость запоминания сложных паролей или ношения с собой дополнительных устройств, что делает процесс аутентификации более удобным и быстрым.

Биометрическая аутентификация обеспечивает более высокий уровень безопасности по сравнению с традиционными методами, поскольку биометрические данные сложно подделать или украсть, что делает их более надежными, чем традиционные методы аутентификации. Например, пароли могут быть украдены, перехвачены или угаданы, а токены могут быть потеряны или скопированы. В случае биометрической аутентификации, уникальные физиологические или поведенческие характеристики человека сложно подделать или скопировать. Это делает биометрическую

аутентификацию более надежной и обеспечивает повышенный уровень безопасности.

Также может помочь предотвратить мошенничество, поскольку биометрическая аутентификация основана на уникальных характеристиках человека, которые трудно имитировать. Подделка отпечатка пальца, лица или других биометрических данных требует значительных усилий и ресурсов, что делает такие попытки мошенничества маловероятными. Это помогает защитить личные данные и предотвратить несанкционированный доступ к системам и устройствам.

Биометрическая аутентификация значительно улучшает взаимодействие с пользователем, устраняя необходимость ввода паролей или использовании токенов. Вместо того, чтобы запоминать и вводить сложные пароли или носить с собой дополнительные устройства, пользователи могут использовать свои уникальные биометрические данные для подтверждения своей личности. Это упрощает процесс аутентификации, делает его более удобным и интуитивно понятным для пользователей.

Однако, несмотря на свои многочисленные преимущества, биометрическая аутентификация также связана с определенными проблемами, которые следует учитывать при ее использовании. Одной из основных проблем является вопрос конфиденциальности биометрических данных. Отпечатки пальцев, данные о лице, радужная оболочка глаза, голос и другие биометрические параметры являются крайне чувствительной личной информацией, подверженной риску утечки или злоупотребления. Поэтому необходимы строгие меры по защите и безопасному хранению этих данных в соответствии с законами и нормами конфиденциальности.

Другой важной проблемой является точность биометрических систем. Несмотря на их высокую эффективность, они могут допускать как ложные срабатывания, так и ложные отказы. Это может быть обусловлено различными факторами, такими как качество биометрических данных, условия окружающей среды или изменения внешности. Некоторые физиологические особенности могут затруднять точное распознавание, что приводит к ошибкам в процессе аутентификации.

Кроме того, биометрические системы аутентификации могут быть уязвимы для различных атак. Например, атака спуфинга (подделка) может быть проведена путем использования фальшивых биометрических данных, таких как поддельные отпечатки пальцев или маски для лица, чтобы обмануть систему [4]. Также возможна атака подмены, когда злоумышленник заменяет биометрические данные легитимного пользователя. Для защиты от таких атак необходимо использовать дополнительные меры безопасности, такие как многофакторная аутентификация.

И последним, но не менее важным аспектом является стоимость внедрения и обслуживания биометрических систем. Это связано с

приобретением специализированного оборудования, разработкой программного обеспечения, обучением персонала и поддержкой системы. Постоянное обновление и обслуживание также требуют дополнительных затрат. Все эти факторы могут повлечь значительные расходы для организаций или пользователей, внедряющих биометрическую аутентификацию.

Исследователи постоянно совершенствуют технологии биометрической аутентификации, стремясь повысить их надежность и удобство использования. Для успешного применения в таких областях, как финансы, здравоохранение и государственные услуги, требуется тщательное управление и дополнительные меры безопасности.

В целом, биометрическая аутентификация является многообещающим методом проверки личности, который может значительно улучшить процесс аутентификации, обеспечивая удобство и повышенную безопасность для пользователей.

Заключение. Биометрическая аутентификация играет ключевую роль в обеспечении безопасности и защите данных, особенно в сферах, требующих высокий уровень защиты, таких как военные объекты, финансовая и медицинская индустрии и другие критически важные сферы. Дальнейшее развитие этой технологии и учет различных факторов помогут обеспечить успешное применение биометрической аутентификации в различных областях.

Библиографический список:

1. Биометрия. Не скуШно. Не душно: [Электронный ресурс]. URL: https://habr.com/ru/companies/gnivc/articles/768834/ (Дата обращения: 15.02.2024)
2. Брагина Е.К., Соколов С.С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития: [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/sovremennye-metody-biometricheskoy-autentifikatsii-obzor-analiz-i-opredelenie-perspektiv-razvitiya/viewer (Дата обращения: 15.02.2024)
3. Биометрическая аутентификация – обзор и сравнение методов проверки: [Электронный ресурс]. URL: https://cloudnetworks.ru/analitika/biometricheskaya-autentifikatsiya-obzor-i-sravnenie-metodov-proverki/ (Дата обращения: 15.02.2024)
4. Степанов М.О. Социальная инженерия: методы атак и способы предотвращения // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XXVII Международной научно-практической конференции, Москва, 25 января 2024 года. –Москва. Печатный цех, 2024 – с. 35-41. (Дата обращения: 15.02.2024)

5. Биометрия: достоинства и недостатки: [Электронный ресурс]. URL: https://securitymedia.org/info/biometriya-dostoinstva-i-nedostatki.html (Дата обращения: 15.02.2024)

6. Биометрия и информационная безопасность: [Электронный ресурс]. URL: https://safe-surf.ru/users-of/article/659637/ (Дата обращения: 15.02.2024)

УДК 004.056

Степанов Максим Олегович, студент
Мисбахов Нияз Ильясович, студент
Лукьянов Эмиль Радикович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Нагаев Назим Харисович, научный руководитель, старший преподаватель кафедры «Системы информационной безопасности»
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, student
Lukyanov Emil Radikovich, student
Misbachov Niaz Ilyasovich, student
Kazan National Israeli Technical University named A.N. Tupolev-KAI
Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer of the Department of "Information security system"
Kazan National Israeli Technical University named A.N. Tupolev-KAI
Russia, Kazan

Роль обучения и осведомленности персонала в обеспечении информационной безопасности

The role of staff training and awareness in ensuring information security

Аннотация: Данная статья подчеркивает важность обучения персонала в области информационной безопасности в современном информационном обществе. В тексте акцентируется внимание на роли обучения и осведомленности в эффективной стратегии безопасности организации, а также указывается важность регулярного обновления и повторения обучающих программ. В статье рассматриваются различные методы и подходы к обучению и осведомленности, включая проведение тренингов и семинаров, предоставление обучающих материалов, тестирование знаний и навыков, а также роль руководства в поддержке инициатив по обучению персонала. Уделено внимание и законодательству в этой области. Статья подчеркивает, что безопасность информации является общей задачей для всех сотрудников, и только совместными усилиями можно обеспечить защиту данных организации и ее устойчивое развитие.
Ключевые слова: обучение персонала, информационная безопасность, осведомленность, защита данных.
Abstract: This article highlights the importance of training personnel in the field of information security in the modern information society. The text focuses on the

role of training and awareness in an effective security strategy of the organization, and also indicates the importance of regular updating and repetition of training programs. The article discusses various methods and approaches to training and awareness, including conducting trainings and seminars, providing training materials, testing knowledge and skills, as well as the role of management in supporting staff training initiatives. Attention is also paid to legislation in this area. The article emphasizes that information security is a common task for all employees, and only joint efforts can ensure the protection of the organization's data and its sustainable development.
Key words: staff training, information security, awareness, data protection.

В современном информационном обществе, где цифровые технологии проникают во все сферы нашей жизни, обучение и осведомленность персонала по информационной безопасности становятся неотъемлемой частью успешной стратегии безопасности организации. Безопасность информации является ключевым активом, и ее защита требует актуальных знаний и навыков у всех сотрудников. От человеческого фактора зависит многое - от предотвращения атак со стороны злоумышленников до обеспечения соблюдения правил и процедур безопасности. Поэтому инвестиции в обучение и осведомленность персонала являются необходимыми для поддержания безопасности организации и обеспечения ее устойчивого развития.

Однако обучение и осведомленность персонала по информационной безопасности - это не единоразовое мероприятие, а непрерывный процесс [1]. Технологии и угрозы постоянно развиваются, поэтому персонал должен быть в курсе последних трендов и методов защиты информации. Регулярное обновление и повторение обучающих программ помогут поддерживать высокий уровень осведомленности и готовности к действию в случае возникновения инцидентов безопасности.

Кроме того, важно учитывать разнообразие ролей и задач в организации при разработке программ обучения. Различные отделы и должности могут иметь свои специфические потребности в области информационной безопасности. Например, сотрудники отдела IT могут требовать более глубоких знаний о сетевой безопасности и угрозах, связанных с программным обеспечением, в то время как сотрудники отдела маркетинга могут больше заинтересованы в защите персональных данных клиентов. Поэтому обучающие программы должны быть адаптированы под различные роли и потребности персонала.

Роль персонала в обеспечении информационной безопасности организации не ограничивается только IT-специалистами. Каждый сотрудник, независимо от должности, играет ключевую роль в поддержании безопасности информации. Понимание возможных угроз, применение

эффективных методов защиты и соблюдение правил безопасности сокращают вероятность возникновения инцидентов безопасности и обеспечивают надежную защиту конфиденциальных данных организации.

Угрозы для безопасности данных организации можно разделить на две основные категории:

– внутренние;
– внешние.

Внутренние угрозы могут возникнуть из-за непреднамеренных действий сотрудников. Например, случайное разглашение конфиденциальной информации или неправильное использование ресурсов. Поэтому каждый сотрудник должен осознавать важность конфиденциальности информации и соблюдать политику безопасности организации. Это включает ограничение доступа к конфиденциальным данным, использование сложных паролей и регулярное обновление программного обеспечения.

Внешние угрозы, такие как вредоносные программы, фишинг-атаки и социальная инженерия, могут быть направлены на любого сотрудника организации. Поэтому каждый сотрудник должен быть осведомлен о различных видах угроз и знать, как распознавать и предотвращать подобные атаки. Обучение сотрудников о социальной инженерии и умение распознавать подозрительные ситуации помогают избежать попадания в ловушки [2].

Соблюдение политики безопасности и безопасных методов также является важным фактором. Каждый сотрудник должен быть ознакомлен с политикой безопасности организации и строго соблюдать ее. Это включает использование сложных паролей, которые состоят из комбинации букв, цифр и специальных символов, регулярное обновление программного обеспечения, ограничение доступа к конфиденциальной информации и другие практики. Сотрудники также должны быть осведомлены о правилах использования электронной почты, обработки данных и обмена информацией, чтобы предотвратить утечку или несанкционированное распространение информации.

Для эффективного обучения и повышения осведомленности персонала по информационной безопасности организации могут использовать различные методы и подходы.

Одним из основных методов является организация тренингов и семинаров по информационной безопасности, который является важным шагом для обеспечения безопасности данных в организации. Проведение таких мероприятий позволяет достичь нескольких преимуществ.

Во-первых, тренинги и семинары позволяют персоналу получить актуальные знания и навыки в области информационной безопасности.

Участие в таких мероприятиях помогает сотрудникам быть в курсе последних угроз, тенденций и эффективных стратегий защиты данных.

Во-вторых, на тренингах и семинарах сотрудники имеют возможность задать вопросы экспертам и обсудить конкретные ситуации, с которыми они сталкиваются в своей работе. Это помогает разрешить сомнения, получить рекомендации и обменяться опытом с коллегами.

Еще одним методом является предоставление обучающих материалов и руководств, которые помогают сотрудникам улучшить свои знания в области информационной безопасности, предоставляя возможность самостоятельного изучения. Эти ресурсы включают в себя онлайн-курсы, вебинары, руководства и информативные листовки, охватывающие разнообразные темы и форматы обучения [3]. Качественные материалы разрабатываются с учетом потребностей целевой аудитории, представляют привлекательный контент и регулярно обновляются, чтобы отражать последние угрозы и лучшие практики в области информационной безопасности.

После завершения обучения необходимо проводить тестирование знаний и навыков в области информационной безопасности. Это позволит не только оценить эффективность обучающей программы, но и убедиться в усвоении материала сотрудниками. Тестирование после обучения дает возможность подтвердить уровень освоения информации, выявить пробелы и недопонимания, а также помогает адаптировать дальнейший процесс обучения к индивидуальным потребностям персонала [4].

Также необходимо постоянно обновлять и повторять обучающие программы для обеспечения успешной стратегии безопасности. Регулярное обновление гарантирует соответствие современным требованиям и угрозам, а повторение помогает закрепить знания и поддерживать высокий уровень готовности персонала к реагированию на инциденты.

Наконец, важно отметить, что руководство должно выступать в качестве примера и поддерживать инициативы по обучению и осведомленности персонала.

Кроме внутренних инициатив, обучение и осведомленность персонала по информационной безопасности также являются требованиями законодательства. Во многих странах существуют нормативные акты, которые обязывают организации обеспечивать безопасность информации и обучать своих сотрудников.

В России, например, вопросы информационной безопасности регулируются Федеральным законом "Об информации, информационных технологиях и о защите информации". Кроме того, Федеральная служба по техническому и экспортному контролю (ФСТЭК) России разрабатывает и выпускает нормативные документы, включая приказы, которые регулируют требования к информационной безопасности. Один из таких приказов - Приказ ФСТЭК России № 239 «Об утверждении требований по обеспечению

безопасности значимых объектов критической информационной инфраструктуры». В этом приказе устанавливаются требования к содержанию и организации обучения сотрудников по вопросам информационной безопасности.

Нужно помнить, что безопасность информации - это задача каждого сотрудника, и только совместными усилиями можно обеспечить безопасное функционирование организации в цифровом мире.

Заключение. Обучение персонала по информационной безопасности является неотъемлемыми компонентами успешной стратегии обеспечения безопасности в организации. Повышение уровня знаний и осведомленности персонала сокращает риски возникновения инцидентов, улучшает защиту информации и обеспечивает безопасное функционирование организации в современном мире. Это позволяет организации быть готовой к изменяющимся угрозам и эффективно реагировать на них, минимизируя потенциальный ущерб и сохраняя доверие клиентов и партнеров. Инвестиции в эту область являются ключевым элементом и способствуют устойчивому развитию организации в долгосрочной перспективе.

Библиографический список:

7. Повышение осведомленности пользователей по вопросам ИБ: [Электронный ресурс]. URL: https://lib.itsec.ru/articles2/control/povyshenie-osvedomlennosti-polzovateley-po-voprosam-ib (Дата обращения: 12.02.2024)

8. Степанов М.О. Социальная инженерия: методы атак и способы предотвращения // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XXVII Международной научнопрактической конференции, Москва, 25 января 2024 года. –Москва. Печатный цех, 2024 – с. 35-41. (Дата обращения: 12.02.2024)

9. Обучение сотрудников: этапы, методы и правила: [Электронный ресурс]. URL: https://www.insales.ru/blogs/university/kak-obuchat-sotrudnikov (Дата обращения: 12.02.2024)

10. Повышение осведомлённости сотрудников: ваш вклад в безопасность: [Электронный ресурс]. URL: https://www.anti-malware.ru/practice/methods/Raising-employee-awareness-your-contribution-to-safety (Дата обращения: 12.02.2024)

0УДК 004.5

Мисбахов Нияз Ильясович, студент
Степанов Максим Олегович, студент
Лукьянов Эмиль Радикович, студент
Шарипов Рифат Рашатович, научный руководитель,
доцент кафедры «Систем информационной безопасности»
Казанский национальный исследовательский технический университет
им. А.Н. Туполева-КАИ
lukanovemil6@gmail.com
Россия, г. Казань

Stepanov Maxim Olegovich, student
Lukyanov Emil Radikovich, student
Misbachov Niaz Ilyasovich, student
Kazan National Israeli Technical University named A.N. Tupolev-KAI
Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer of the
Department of "Information security system"
Kazan National Israeli Technical University named A.N. Tupolev-KAI
Russia, Kazan

Сравнительный анализ «Система контроля и управления доступа»

Comparative analysis of "Access Control and Management System"

Аннотация: В данной статье проводится обзор и анализируются современные системы контроля и управления доступом. Актуальность данной темы обосновано необходимостью внедрения систем защиты информации в компании занимающиеся персональными данными и конфиденциальной информацией. Для наглядного примера проведён анализ самых популярных систем контроля и управления доступом в Российской Федерации. Представлен список оборудования необходимый для подключения и его стоимость.

Ключевые слова: система контроля и управлением доступа, проектирование, считыватели, замки, исполнительные устройства.

Abstract: This article reviews and analyzes modern access control and management systems. The relevance of this topic is justified by the need to implement information security systems in companies dealing with personal and confidential data. For a clear example, an analysis of the most popular access

control and management systems in the Russian Federation is carried out. A list of equipment required for connection and its cost is presented.

Key words: access control and management system, design, readers, locks, executive devices

СКУД — это аббревиатура, которая означает "Система контроля и управления доступом". Это комплексная система, предназначенная для обеспечения контроля и управления доступом людей на определенные территории, здания или помещения.

Основная цель СКУД - обеспечить безопасность и ограничить доступ только уполномоченных лиц. С помощью СКУД можно установить и контролировать права доступа, записывать информацию о проходах, а также управлять системой охранной сигнализации.

СКУД Parsec:

Система контроля и управления доступом Parsec разработана для обеспечения безопасности на объектах различного масштаба - от малых предприятий до комплексов зданий. Кроме того, она поддерживает возможности охранной и пожарной сигнализации.

Основным компонентом системы является контроллер NC-60K.M, который выполняет центральные функции. Каждый контроллер обслуживает одну точку прохода и отвечает за контроль охранной сигнализации в соответствующем помещении.

Контроллеры поставляются в металлических корпусах с встроенным источником питания, который обеспечивает работу как системной электроники, так и замков. На рисунке 1 представлен контроллер серии NC-60K.M

Рисунок 1. - Контроллер Parsec серии NC-60K.M

СКУД РУСГУАРД

СКУД РусГард предлагает комплексные решения для офисов и учреждений, которые обеспечивают надежную защиту от несанкционированного доступа, управление доступом в помещения, автоматизацию контроля рабочего времени и трудовой дисциплины.

Контроллеры РусГард выполняют анализ кодов доступа и принимают решение о разрешении или запрете прохода сотрудников на территорию с ограниченным доступом в соответствии с их правами доступа. Они также имеют возможность управления электромеханическими замками дверей, турникетами и автоматическими шлагбаумами.

Контроллер СКУД ACS-102-CE-B (WF) отличается наличием встроенного WiFi модуля MicRotic mAP2nD. Настройка WiFi модуля MicRotic mAP2nD осуществляется путем подключения ПК к порту LAN. Конфигурация контроллера производится через веб-интерфейс. В веб-интерфейсе контроллеров доступны номера карт и ФИО сотрудников. Кроме того, есть возможность ограничить доступ по помещениям, времени и статусу. Рисунок 2 показывает данный контроллер.

Рис. 2. Контроллер СКУД ACS-102-CE-B (WF)

СКУД Legos:

Система контроля и управления доступа Legos — это универсальная платформа, которая объединяет функции самостоятельного и сетевого контроля доступа. Она работает с центральным управляющим устройством (компьютером) под управлением оператора, но также может перейти в автономный режим в случае сбоя центрального устройства, сетевого оборудования или потери связи. На рынке доступно пять серий контроллеров Legos, каждая из которых предназначена для определенных потребностей клиентов. Серия L3 универсальна, L4 - бюджетной, L5 - классическая, L6 - обеспечивает охранно-пожарную сигнализацию и управление пожаротушением, а L8 - сетевая. Давайте подробнее рассмотрим контроллеры из серии L5, специально разработанные для систем контроля и управления доступом на средних и крупных объектах. Пример такого контроллера представлен на рисунке 3.

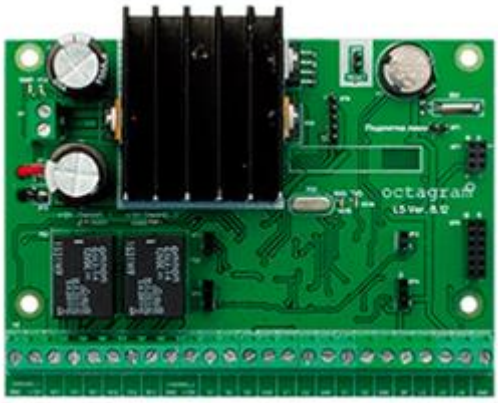


Рис. 3. - Контроллер Legos серии L5

Каждая модель устройства в данной серии способна управлять одной точкой доступа и контролировать набор охранно-пожарных извещателей. Все устройства этой серии оборудованы встроенной энергонезависимой памятью на 4000 или 32000 пользователей/событий. Они также имеют функцию "Antipassback" для предотвращения повторного прохода, самостоятельно контролируют питание и уровень заряда аккумулятора, а также могут выполнять аварийное открытие двери.

Сравнительный анализ выбранных систем контроля и управения доступом (СКУД) по некоторым значимым критериям (табл.1):

	Parsec	РУСГУАРД	Legos
Контроллеры	NC-60K.M	ACS-102-CE-B (WF)	L5
Количество ключей	8000	64000	4000
Количество событий в памяти контроллера	32 000	60000	32000
Напряжение питания	220 В	220 В	220 В
Интерфейс считывающих устройств	Touch Memory / Wiegand-26	Wiegand-26/37/44/52, Touch Memory	Touch Memory / Wiegand-26 (через TWT)
Интерфейс связи с компьютером	Ethernet, RS-485	WiFi, CAN-HS, Ethernet	LBUS, RS-232
Количество считывателей	2	2	2
Количество подключаемых контроллеров на (АРМ)	до 1024	неограниченно	до 256
Наличие Wifi-модуль	-	MicRotic mAP2nD	-
Срок службы	5 лет	5 лет	8 лет
Считыватели	PR-P09	RDR-102-EH-G	PLR3
Дальность считывания	4 см	6-14 см	6 см

Интерфейс связи с контроллером	Touch Memory / Wiegand-26	Wiegand 26, Dallas Touch Memory	Touch Memory / Wiegand-26

Табл.1 Сравнительный анализ СКУД

Выбор СКУД защищаемого объекта

После проведения сравнительного анализа СКУД разных производителей, было обнаружено, что СКУД РусГуард обладает рядом преимуществ, которые делают ее наиболее предпочтительной системой для защищаемого объекта:

- СКУД РусГуард обеспечивает высокий уровень безопасности и контроля доступа. Она имеет мощные алгоритмы шифрования и аутентификации, а также поддерживает различные методы идентификации, включая биометрические данные, карты доступа и пин-коды. Это позволяет эффективно ограничивать доступ к объекту только авторизованным лицам.
- СКУД РусГуард обладает гибкой и масштабируемой архитектурой, что позволяет ее легко настраивать и адаптировать под конкретные потребности защищаемого объекта. Она поддерживает управление несколькими точками доступа, интеграцию с другими системами безопасности и возможность расширения функциональности в будущем.

Кроме того, СКУД РусГуард предлагает удобный и интуитивно понятный пользовательский интерфейс, что упрощает управление и мониторинг системы. Она также обладает надежной и стабильной работой, что гарантирует бесперебойную работу системы контроля доступа.

Исходя из всех этих факторов, можно сделать вывод, что СКУД РусГуард является наиболее предпочтительной системой для защищаемого объекта, так как она обеспечивает высокий уровень безопасности, гибкость, удобство использования и надежность.

Состав оборудования СКУД РусГуард:

- Контроллеры СКУД ACS-102-CE-B (WF);
- Считыватели RDR-102-EH-G;
- электромеханические, электромагнитные замки и кнопки выхода из помещения;
- дверные доводчики.
- ПО RusGuard Soft в виде стандартного пакета с дополнительными модулями.
- На ПК должна быть установлена лицензионная версия ОС семейства Microsoft Windows.

Рассчитаем стоимость оборудования для установки СКУД, информация приведена в таблице 2.

№	Наименование	Кол-во единиц	Стоимость единицы, руб.	Сумма, руб.
1	АРМ+ ОС Windows 10	1	32000	32000
2	Контроллер ACS-102-CE-B (WF)	14	21000	294000
3	Считыватель RDR-102-EH-G	26	2940	76440
4	Электромеханический замок EL566 ABLOY	23	7600	174800
5	Электромагнитный замок TS-ML300	3	3860	11580
6	Доводчик двери	26	1510	39260
7	Кнопка выхода	26	310	8060
8	Точка доступа TP-LINK TL-WA801ND	2	1400	2800
9	ALFA Battery AGM	14	600	8400
	Итого			**647340**

Табл. 2. Стоимость покупки оборудования

Заключение. В заключение, проведенный сравнительный анализ систем контроля и управления доступом (СКУД) позволил рассмотреть различные аспекты и характеристики этих систем.

Анализ показал, что все модели данной серии СКУД обладают высокой эффективностью и надежностью в обеспечении безопасности объектов. Встроенная энергонезависимая память от 16000 до 60000 пользователей/событий обеспечивает достаточное пространство для хранения информации о доступе и событиях.

В целом, сравнительный анализ систем контроля и управления доступом позволяет выбрать наиболее подходящую модель СКУД, учитывая требования безопасности и функциональные потребности объекта. Эти системы играют важную роль в обеспечении безопасности и контроле доступа, способствуя эффективной работе и защите информационных ресурсов. В контексте обеспечения безопасности предприятия также значимы системы пожарной сигнализации, которые предотвращают незаконное вторжение злоумышленников, исключая возможность использования СКУД, и обеспечивают оперативное оповещение о возгораниях. После внедрения системы контроля и управления доступом в компанию появились следующие возможности: разграничение доступа, контроль доступа по территории предприятия для сотрудников и автоматизация контроля трудовой деятельности.

Библиографический список:

1. Фаткулин, А. Н. Анализ современных систем контроля и управления доступом / А. Н. Фаткулин, Е. Н. Окладникова, Е. Н. Сухарев // Актуальные проблемы авиации и космонавтики. – 2011. – Т. 1, № 7. – С. 263-264.

2. Патент № 2643898 C1 Российская Федерация, МПК G07C 9/00. Система контроля и управления доступом с использованием мобильного телекоммуникационного устройства: № 2016145370: заявл. 18.11.2016: опубл. 06.02.2018 / Т. Ю. Шейкин.

3. Лукьянов Э. Р. Разработка системы контроля управления доступом в компании Арсенал // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XXV Международной научно-практической конференции, Москва, 17 ноября 2023 года. –Москва. Печатный цех, 2023 – С. 202-208.

4. Юсупов, Б. З. Разработка лабораторного стенда охранно-пожарной сигнализации по дисциплине технические средства охраны / Б. З. Юсупов, А. М. Мартынов // Актуальные проблемы науки и образования в условиях современных вызовов : Сборник материалов XIX Международной научно-практической конференции, Москва, 21 марта 2023 года. – Москва: Печатный цех, 2023. – С. 80-91.

5. Юсупов, Б. З. Методика проведения лабораторных работ на стенде «ОПС Астра-812pro» по дисциплине «Технические средства охраны» / Б. З. Юсупов, А. М. Мартынов, Р. Р. Шарипов // Информационные технологии в науке, промышленности и образовании. Молодежный научный форум : Сборник трудов Всероссийской научно-технической конференции, Ижевск, 25–26 мая 2023 года. – Ижевск: Ижевский государственный технический университет имени М.Т. Калашникова, 2023. – С. 476-479.

6. Юсупов Б. З. Разработка лабораторного стенда охранно-пожарной сигнализации по дисциплине технические средства охраны. – 2021.

7. Макаров С.П. Разработка программного комплекса регистра сдвига с линейной обратной связью /С.П. Макаров, А.А. Кассирова // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XXV Международной научно-практической конференции, Москва, 17 ноября 2023 года. –Москва. Печатный цех, 2023 – С. 27-34.

8. Кассирова А.А. Исследование алгоритма «Берлекэмпа-Месси» на простых регистрах сдвига с линейной обратной связью / А.А. Кассирова, С.П. Макаров// Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XXV Международной научно-практической конференции, Москва, 17 ноября 2023 года. –Москва. Печатный цех, 2023 – С. 217-227.

9. Шарипов, Р. Р. Исследование электрических параметров пороговых извещателей / Р. Р. Шарипов, Б. З. Юсупов // Программные системы и вычислительные методы. – 2023. – № 3. – С. 29-47. – DOI 10.7256/2454-0714.2023.3.43682.

10. Юсупов, Б. З. Разработка учебного стенда охранно-пожарной системы для обучения студентов / Б. З. Юсупов // Программные системы и вычислительные методы. – 2023. – № 2. – С. 40-48. – DOI 10.7256/2454-0714.2023.2.43552.

11. Юсупов Б. З. Разработка методики проведения лабораторных работы на стенде «ОПС Астра-713» по дисциплине технические средства охраны. – 2021.

12. Серебряков М.А. Исследование лабораторного помещения на наличие устройств акустоэлектрического преобразования // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XXV Международной научно-практической конференции, Москва, 17 ноября 2023 года. –Москва. Печатный цех, 2023 – С. 40-44.

13. Серебряков М.А. Разработка лабораторный стенда для измерений акустоэлектрического канала // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XXV Международной научно-практической конференции, Москва, 17 ноября 2023 года. –Москва. Печатный цех, 2023 – С. 45-51.

14. Шарипов, Р. Р. Исследования скорости передачи данных в PLC сети в учебной лаборатории / Р. Р. Шарипов, А. Ф. Фатхелисламов // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 55-60.

15. Мартынов, А. М. Разработка учебного стенда системы видео контроля / А. М. Мартынов // Программные системы и вычислительные методы. – 2023. – № 4. – С. 102-114. – DOI 10.7256/2454-0714.2023.4.69055.

УДК 004.056

Степанов Максим Олегович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ

Нагаев Назим Харисович, научный руководитель, старший преподаватель кафедры «Системы информационной безопасности»
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, student
Kazan National Research Technical University named after A.N. Tupolev-KAI

Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer at the Department of Information Security Systems
Kazan National Research Technical University named after A.N. Tupolev-KAI
Russia, Kazan

Обзор SSL-сертификатов и их роль в безопасности веб-сайтов

Overview of SSL Certificates and their role in website security

Аннотация: Данная статья представляет обзор SSL-сертификатов и их важную роль в обеспечении безопасности веб-сайтов. Начиная с принципов работы SSL, она рассматривает различные аспекты защиты, предоставляемой этими сертификатами, включая базовое шифрование данных и дополнительные уровни доверия. Обсуждаются особенности каждого типа сертификатов, их применение и важность для обеспечения безопасного соединения между серверами и браузерами. Эта статья поможет читателям понять различия между типами SSL-сертификатов и выбрать подходящий для своих потребностей уровень защиты.
Ключевые слова: SSL-сертификат, типы, конфиденциальность, целостность, информационная безопасность.
Abstract: This article provides an overview of SSL certificates and their important role in securing websites. Starting with the principles of SSL, it examines various aspects of the protection provided by these certificates, including basic data encryption and additional levels of trust. The specifics of each type of certificate, their application and importance for ensuring a secure connection between servers and browsers are discussed. This article will help readers understand the

differences between the types of SSL certificates and choose the appropriate level of protection for their needs.

Key words: SSL certificate, types, confidentiality, integrity, information security.

С каждым днем число онлайн-угроз и попыток хакерских атак увеличивается, делая безопасность в интернете одним из приоритетов как для пользователей, так и для владельцев веб-ресурсов. В связи с этим SSL-сертификаты становятся не просто необходимым элементом, а надежным барьером, защищающим конфиденциальные данные и обеспечивающим доверие пользователей.

SSL-сертификат - это цифровой сертификат, который подтверждает подлинность веб-сайта и создает зашифрованное соединение между веб-сайтом и браузером.

SSL-сертификаты защищают идентификационные данные удаленного подключения и делают онлайн-взаимодействия конфиденциальными, гарантируя, что никто, кроме отправителя и получателя, не сможет прочитать или изменить содержимое, передаваемое по защищенному соединению. SSL-сертификат действует как паспорт для подтверждения личности владельца веб-сайта и как ключ для обеспечения безопасности пользовательских данных с помощью надежного шифрования [1].

Принцип работы SSL (Secure Sockets Layer) сертификатов основан на криптографии с открытым ключом (асимметричной криптографии). Вот как это происходит [2]:

1. Запрос на соединение: Когда пользователь пытается подключиться к защищенному веб-сайту, его браузер отправляет запрос на соединение с сервером.
2. Отправка сертификата сервера: Сервер отправляет свой SSL сертификат браузеру.
3. Проверка подлинности сертификата: Браузер проверяет подлинность сертификата с помощью удостоверяющего центра (CA), чтобы убедиться, что он действительно принадлежит серверу, с которым пользователь пытается соединиться.
4. Формирование общего секретного ключа: Браузер генерирует случайный секретный ключ и использует открытый ключ, предоставленный в сертификате сервера, для его зашифрования и отправки обратно на сервер.
5. Расшифровка секретного ключа на сервере: Сервер использует свой закрытый ключ, чтобы расшифровать секретный ключ, полученный от браузера.
6. Установка защищенного соединения: Теперь и браузер, и сервер имеют общий секретный ключ, который они могут использовать для шифрования и расшифрования данных, передаваемых между ними во время

сеанса связи. Это защищенное соединение обеспечивает конфиденциальность и целостность передаваемой информации.

Принцип работы SSL сертификатов позволяет защитить передаваемые данные от прослушивания и подмены злоумышленниками, обеспечивая безопасное взаимодействие между сервером и браузером.

После разбора принципа работы SSL сертификатов, важно обратить внимание на различные типы таких сертификатов [3].

SSL-сертификаты с проверкой домена (DV SSL) представляют собой базовый уровень сертификатов безопасности, обеспечивающих основное шифрование данных между веб-сайтом и его посетителями. При запросе сертификата DV SSL процесс проверки ограничивается только подтверждением владения доменом, на котором будет использоваться сертификат.

Владелец веб-сайта должен предоставить доказательства того, что контролирует или имеет доступ к управлению доменным именем. Этот процесс обычно включает в себя отправку электронного сообщения на адрес электронной почты, связанный с доменом, либо размещение специального файла на веб-сайте для подтверждения владения им. После завершения этого процесса выдается сертификат, который обеспечивает базовое шифрование данных при передаче между веб-сайтом и его посетителями.

Сертификаты DV SSL отображаются в адресной строке браузера как замок и префикс "HTTPS", что указывает на использование безопасного соединения. Однако, они не содержат дополнительной информации о владельце веб-сайта, такой как название компании или юридический адрес. Такие сертификаты обычно используются для небольших или личных веб-сайтов, которым не требуется сбор конфиденциальной информации, такой как данные кредитных карт или личные данные пользователей.

Сертификаты с проверкой организации (OV SSL) представляют собой высокоуровневые SSL-сертификаты, обеспечивающие дополнительный уровень доверия и безопасности для веб-сайтов. При запросе сертификата OV SSL происходит проверка как самого домена, так и самой организации, заказывающей сертификат. Этот процесс включает проверку подлинности и юридического статуса организации, а также ее физического местоположения.

После успешной проверки выдается сертификат, который включает в себя информацию о компании, владеющей доменом, такую как название компании и юридический адрес. Этот тип сертификата обеспечивает шифрование передаваемых данных между веб-сайтом и его посетителями, а также гарантирует, что информация о компании была проверена по международным стандартам безопасности.

Сертификаты расширенной проверки (EV SSL) представляют собой наиболее дорогой вариант SSL-сертификатов. Они применяются в основном на веб-ресурсах высшего класса, где происходит сбор данных и проведение

онлайн-транзакций. После установки сертификата расширенной проверки в адресной строке браузера отображается замок, что помогает различить этот ресурс от потенциально опасных. На сайтах с таким сертификатом в адресной строке также указывается название компании-владельца и страна. Чтобы получить сертификат EV SSL, владелец сайта должен пройти процедуру проверки личности, подтверждающую его право на использование доменного имени. Данный тип сертификата основном используется в банковской сфере.

Wildcard SSL-сертификаты - это специальный тип SSL-сертификатов, которые предназначены для защиты базового домена и всех его поддоменов при помощи одного сертификата. Они используются для обеспечения безопасного соединения между пользователем и сервером для всех поддоменов, которые соответствуют шаблону.

Например, если есть домен example.com, и необходимо защитить все его поддомены, такие как login.example.com, mail.example.com, и т.д., можно использовать один Wildcard SSL-сертификат для всех них. Это позволяет сэкономить время и ресурсы на управлении сертификатами для каждого поддомена отдельно.

Основное преимущество SSL-сертификатов с подстановочными знаками (Wildcard SSL) заключается в их экономической эффективности. Они позволяют защитить основной домен и все его поддомены с помощью одного сертификата, что обеспечивает значительную экономию средств по сравнению с использованием отдельных сертификатов для каждого поддомена.

Многодоменные SSL-сертификаты (MDC) позволяют защитить несколько различных доменов и/или поддоменов с различными именами при помощи одного сертификата. Они не ограничены только поддоменами базового домена, как это делает сертификат с подстановочными знаками, а позволяют защитить разные домены с разными именами. Например, один многодоменный сертификат может защищать example.com, example.net, blog.example.org и т. д.

Сертификаты унифицированных коммуникаций (UCC) также являются многодоменными и предназначены для защиты нескольких доменов с разными именами. Эти сертификаты разработаны специально для удовлетворения потребностей организаций, использующих серверы Microsoft Exchange или Office Communications, они обеспечивают удобство и снижают расходы за счет защиты нескольких доменов с помощью одного сертификата.

Заключение. SSL-сертификаты являются важным инструментом обеспечения безопасности в интернете, защищая передаваемые данные от прослушивания и подмены. Они обеспечивают подлинность веб-сайтов и создают зашифрованное соединение между сервером и браузером пользователя, обеспечивая конфиденциальность и целостность информации.

Отличия между различными типами SSL-сертификатов, такими как DV SSL, OV SSL, EV SSL, Wildcard SSL, MDC и UCC, позволяют выбирать наиболее подходящий вариант в зависимости от потребностей конкретного проекта.

Библиографический список:

1. What Is an SSL Certificate? Definition and Guide: [Электронный ресурс]. URL: https://www.shopify.com/ng/blog/what-is-ssl-certificate (Дата обращения: 24.02.2024)
2. SSL-сертификат: что это, зачем нужен и как установить: [Электронный ресурс]. URL: https://education.yandex.ru/journal/chto-takoe-ssl-sertifikat-i-kak-ego-ustanovit (Дата обращения: 24.02.2024)
3. 6 Types of SSL Certificates for Your Website: [Электронный ресурс]. URL: https://www.liquidweb.com/blog/ssl-certificates/ (Дата обращения: 24.02.2024)
4. Types of SSL Certificates: Which One Is Right for Your Site?: [Электронный ресурс]. URL: https://kinsta.com/blog/types-of-ssl-certificates/ (Дата обращения: 24.02.2024)
5. What is an SSL certificate?: [Электронный ресурс]. URL: https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/ (Дата обращения: 24.02.2024)

0УДК 004.5

Степанов Максим Олегович, студент
Лукьянов Эмиль Радикович, студент
Мисбахов Нияз Ильясович, студент
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ
Россия, г. Казань

Шарипов Рифат Рашатович, научный руководитель,
доцент кафедры «Систем информационной безопасности»
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, student
Lukyanov Emil Radikovich, student
Misbakhov Niyaz Ilyasovich, student
Kazan National Research Technical University named after. A.N. Tupolev-KAI
Russia, Kazan

Rifat Rasatovich Sharipov, scientific supervisor,
Associate Professor of the Department of Information Security Systems
Kazan National Research Technical University named after. A.N. Tupolev-KAI
Russia, Kazan

Разработка охранно-пожарной системы для компании Вавилон

Development of a security and fire system for the Babylon company

Аннотация: Научная статья представляет собой разработку и обширное исследование, нацеленное на обзор охранно-пожарной системы, а также разработку и установку системы в компанию «Вавилон». Рассматриваются актуальные вопросы и законодательные требования, используемые при создании таких систем. Для наглядного примера представлен проект внедрения охранно-пожарной системы в определенную компанию. Предоставляются подробный состав оборудования используемый для разработки в компании охранно-пожарной системы (ОПС). На схематическом изображении проекта показано размещение компонентов системы.

Ключевые слова: охранно-пожарная система, система охранной сигнализации, система пожарной сигнализации, извещатель, приемно-контрольный пульт, датчик, устройство, технические средства.

Abstract: The scientific article is a development and an extensive study aimed at reviewing the security and fire alarm system and developing and installing a system for the “Babylon” company. Current issues and legislative requirements used in creating such systems are considered. As a clear example, a project for the implementation of a security and fire alarm system in a specific company is presented. A detailed list of equipment used to develop a security and fire alarm system (OPS) company is provided. A schematic image of the project shows the location of system components.

Key words: Security and fire alarm system, security alarm system, fire alarm system, detector, control panel, sensor, device, technical means.

Основная цель охранной пожарной сигнализации является спасение жизней при пожаре и минимизация материального ущерба компании. Благодаря своевременному быстрому обнаружению очага возгорания и оперативной его ликвидации, можно существенно сократить расходы на восстановление испорченного имущества.

В типовой состав охранной пожарной сигнализации должны входить следующие технические средства [1]:

- Датчики дыма и температуры
- Контрольная панель
- Устройства оповещения (сирена, световые сигналы)
- Устройства пожаротушения (огнетушители, спринклеры)
- Устройства управления доступом (магнитные замки, турникеты)

Основными задачами использования охранной пожарной сигнализации на предприятии являются [2]:

- постоянный контроль и защита объекта от несанкционированного проникновения;
- постоянный контроль периметра внутри объекта на предмет возгорания;
- оповещение и своевременная эвакуация людей из здания

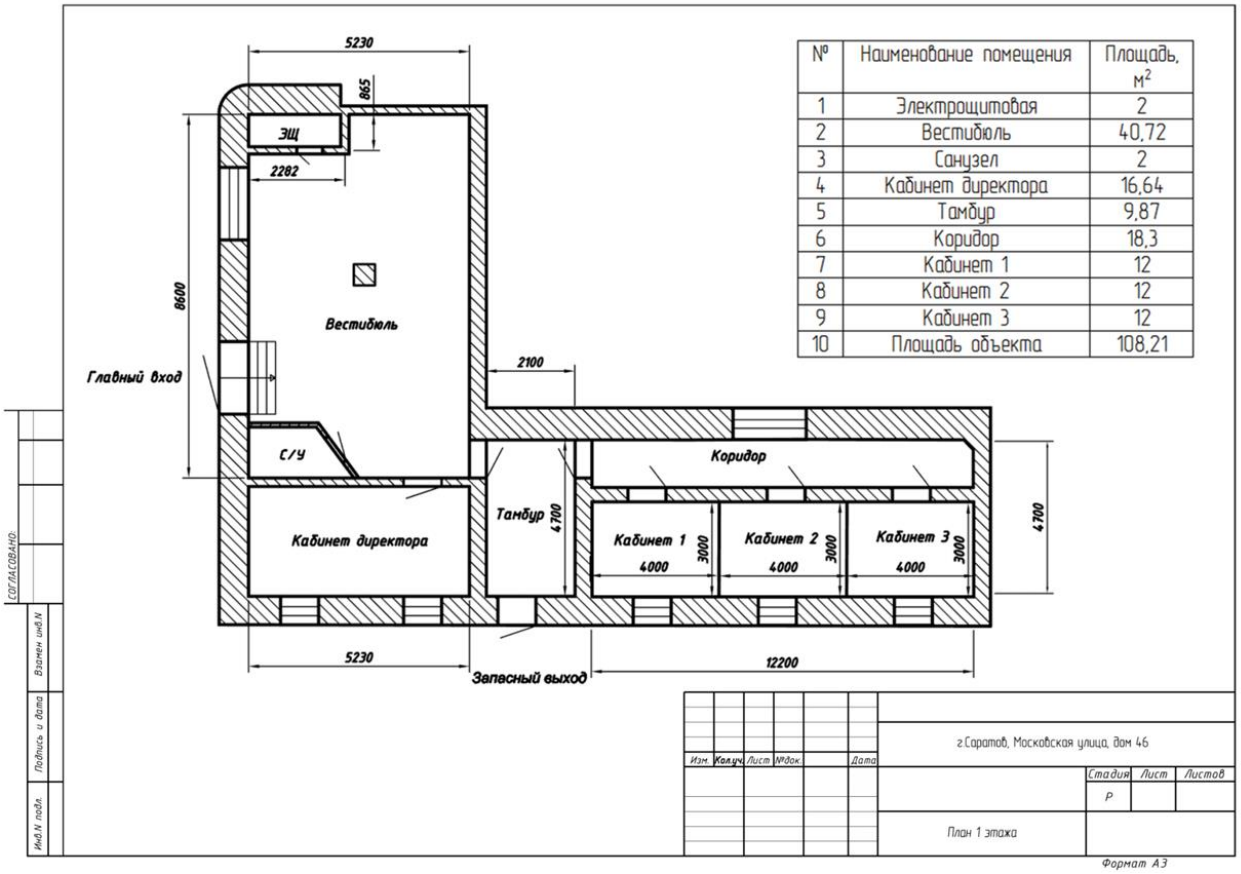
Установка, монтаж и обслуживание охранно-пожарной сигнализации регламентируются следующими законодательными актами [3]:

- ГОСТ 26342-84 (перечень и описание всех типов ОПС);
- ФЗ № 123-ФЗ от 22.07.2008 (техрегламент на проектирование и монтаж ОПС);
- нормы пожарной безопасности НПБ 110-03 (актуальны для объектов, сданных в эксплуатацию до 01.05.2009);
- свод правил СП 13130.2009, регламентирующий размещение охранно-пожарной сигнализации в проектируемых, строящихся, проходящих капитальный ремонт или реконструкцию зданиях;

- ГОСТ 701-2008, содержащий требования к проектной документации;
- нормы пожарной безопасности НПБ 58-97 (нормативы монтажа и испытаний адресной пожарной сигнализации);
- свод правил СП 76.13330.2016, определяющий порядок прокладки и технические параметры кабелей;
- руководящий документ РД 78.145-93, регламентирующий работы по монтажу охранно-пожарной сигнализации, приемку и оформление документации;
- руководящий документ РД 25.964-90, регламентирующий техническое обслуживание и ремонт ОПС.

В данном проекте в качестве объекта, для которого необходимо спроектировать охранно-пожарную систему, выступает одноэтажное здание компании ООО «Вавилон». Здание расположено по адресу: г. Саратов, Московская улица, дом 46.

Это капитальное здание, которое принадлежит компании, имеет стены толщиной 25 см из кирпича с добавлением 4 см штукатурки с каждой стороны. Потолки здания имеют высоту 3.5 метра. Охрана здания обеспечивается наемным персоналом с 8:30 утра до 20:00 вечера. Рабочее время компании с 9:00 утра до 19:00 вечера. План этажа представлен на рисунке 1.



№	Наименование помещения	Площадь, м²
1	Электрощитовая	2
2	Вестибюль	40,72
3	Санузел	2
4	Кабинет директора	16,64
5	Тамбур	9,87
6	Коридор	18,3
7	Кабинет 1	12
8	Кабинет 2	12
9	Кабинет 3	12
10	Площадь объекта	108,21

Рис. 1. План защищаемой компании

Состав оборудования

1.Устройство шлейфовое контрольное УШК-01;

2.Блок приемно-контрольный охранно-пожарный Сигнал-10;

3.Резервированный источник питания РИП-12;

4.Извещатель пожарный ручной адресный ИПР 513-3ПАМ;

5.Пульт контроля и управления охранно-пожарный С2000М;

6.Оповещатель световой табличный С2000-ОСТ;

7.Извещатель пожарный дымовой оптико-электронный адресный ДИП-34ПА-03;

8.Оповещатель охранно-пожарный звуковой С2000-ОПЗ;

9.Извещатель охранный магнитноконтактный адресный С2000-СМК;

10.Извещатель охранный объемный оптико-электронный С2000-ИК;

11.Извещатель охранный поверхностный звуковой адресный С2000-СТ;

12.Контроллер двухпроводный линии связи С2000-КДЛ;

13.Выносной светодиод для индикации постановки объекта на охрану;

14.Устройство Touch Memory. План размещения пожарной системы и оповещения о пожаре размещён на рисунке 2 и 3.

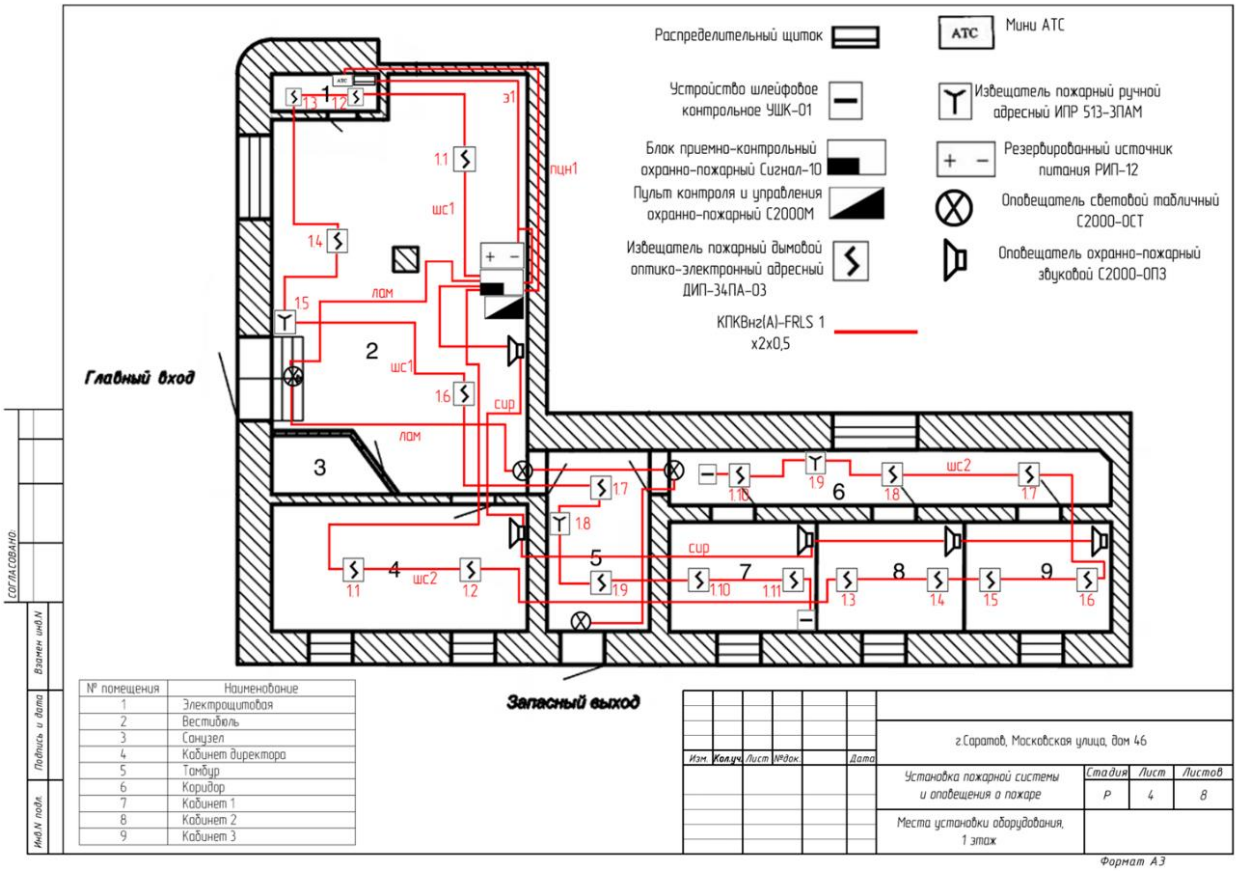


Рис. 2. План расположения пожарной системы и оповещения о пожаре

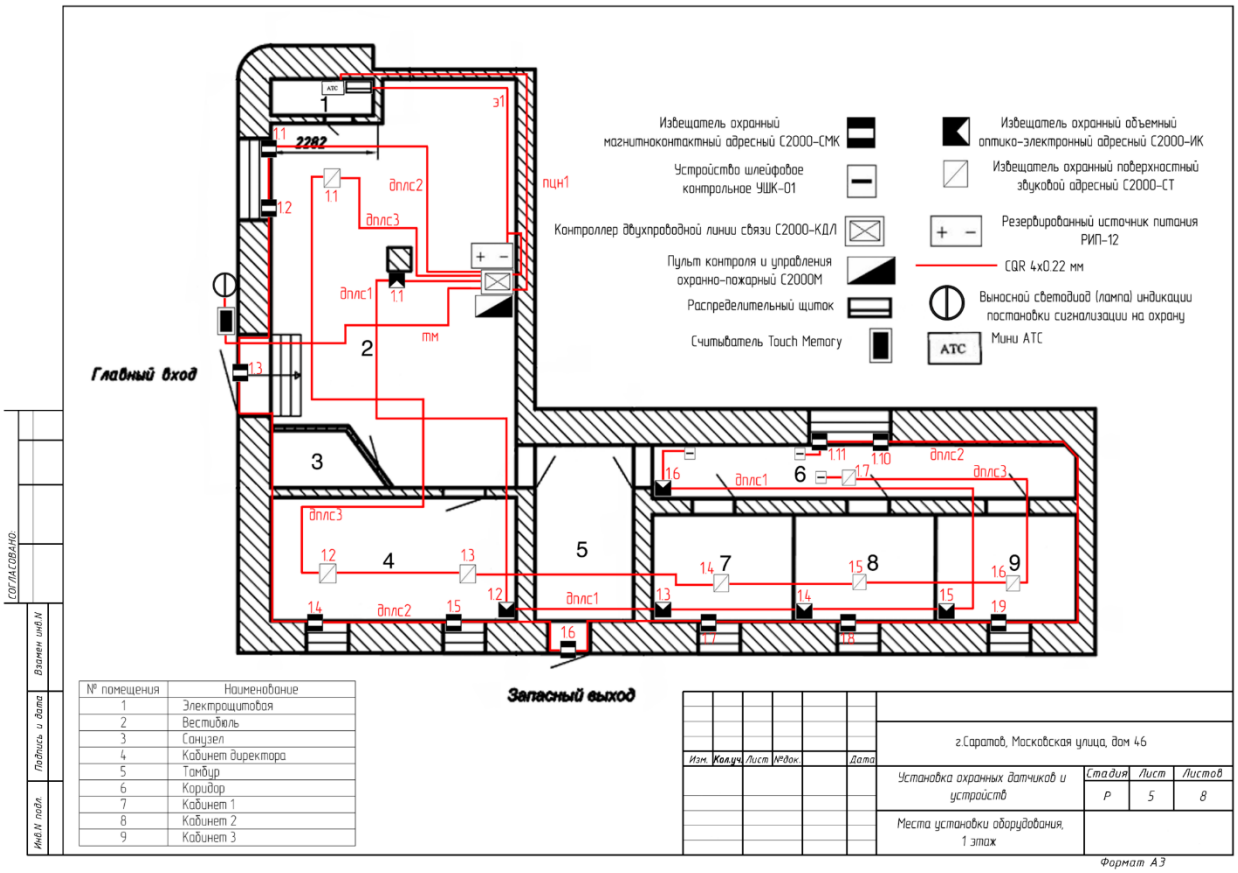


Рис. 3. План расположения пожарной системы и оповещения о пожаре

Расчет стоимости технического оборудования в данном проекте можно увидеть в таблице**Ошибка! Источник ссылки не найден.**.

№	Наименование	Кол-во	Цена за единицу (руб)
1	Контроллер двухпроводный линии связи С2000-КДЛ	1 шт	2 484
2	Блок приемно-контрольный охранно-пожарный Сигнал-10	1шт	2 394
3	Резервированный источник питания РИП-12	1 шт	5 381
4	Извещатель пожарный ручной адресный ИПР 513-3ПАМ	3 шт	534
5	Пульт контроля и управления охранно-пожарный С2000М	1 шт	7 371
6	Оповещатель световой табличный С2000-ОСТ	4 шт	873
7	Оповещатель звуковой С2000-ОПЗ	5 шт	1 475
8	Извещатель пожарный дымовой оптико-электронный адресный ДИП-34ПА-03	21 шт	756
9	Извещатель охранный магнитноконтактный адресный С2000-СМК	11 шт	319
10	Извещатель охранный объемный оптико-электронный С2000-ИК	6 шт	1 029
11	Извещатель охранный поверхностный звуковой адресный С2000-СТ	7 шт	741
12	Устройство шлейфовое контрольное УШК-01	5 шт	193

13	Выносной светодиод для индикации постановки объекта на охрану	1 шт	350
14	Устройство Touch Memory «Считыватель 3»	1 шт	391
15	Кабель для систем сигнализации CQR 4x0.22 мм	200 м	24 руб/м
16	Кабель для систем ОПС и СОУЭ КПКВнг(А)-FRLS 1x2x0,5	230 м	20 руб/м
Итого:	71 951 рублей		

Табл. 2. Стоимость покупки оборудования

После внедрения охранной пожарной сигнализации в компанию появились следующие возможности: она помогает быстро обнаружить возгорание и принять меры по его устранению.

Заключение. Данная научная статья представляет себя как важный вклад в организацию и внедрение охранной пожарной сигнализации. Данная система может способствовать оптимизации безопасности предприятии в целом. В статье проводится разработка охранной пожарной сигнализации в компанию «Вавилон» также предоставляется план установленного оборудования, а также и его состав.

Библиографический список:

1. Фаткулин, А. Н. Анализ современных систем контроля и управления доступом / А. Н. Фаткулин, Е. Н. Окладникова, Е. Н. Сухарев // Актуальные проблемы авиации и космонавтики. – 2011. – Т. 1, № 7. – С. 263-264.

2. Патент № 2643898 C1 Российская Федерация, МПК G07C 9/00. Система контроля и управления доступом с использованием мобильного телекоммуникационного устройства: № 2016145370: заявл. 18.11.2016: опубл. 06.02.2018 / Т. Ю. Шейкин.

3. Лукьянов, Э. Р. Разработка системы контроля управления доступом в компании Арсенал / Э. Р. Лукьянов // Актуальные проблемы науки и образования в условиях современных вызовов (шифр –МКАП 25) : Сборник материалов XXV Международной научно-практической конференции, Москва, 17 ноября 2023 года. – Москва: Печатный цех, 2023. – С. 202-209.

4. Шарипов, Р. Р. Исследование электрических параметров пороговых извещателей / Р. Р. Шарипов, Б. З. Юсупов // Программные системы и вычислительные методы. – 2023. – № 3. – С. 29-47. – DOI 10.7256/2454-0714.2023.3.43682.

5. Юсупов, Б. З. Разработка учебного стенда охранно-пожарной системы для обучения студентов / Б. З. Юсупов // Программные системы и

вычислительные методы. – 2023. – № 2. – С. 40-48. – DOI 10.7256/2454-0714.2023.2.43552.

6. Юсупов, Б. З. Методика проведения лабораторных работ на стенде «ОПС Астра-812pro» по дисциплине «Технические средства охраны» / Б. З. Юсупов, А. М. Мартынов, Р. Р. Шарипов // Информационные технологии в науке, промышленности и образовании. Молодежный научный форум : Сборник трудов Всероссийской научно-технической конференции, Ижевск, 25–26 мая 2023 года. – Ижевск: Ижевский государственный технический университет имени М.Т. Калашникова, 2023.

УДК 004.056

Степанов Максим Олегович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Нагаев Назим Харисович, научный руководитель, старший преподаватель кафедры «Системы информационной безопасности»
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, Student
Lukyanov Emil Radikovich, Student
Misbachov Niaz Ilyasovich, Student
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI
Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer of the department "Si" "Information security system"
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI
Russland, Kasan

Больше, чем просто информация: сила OSINT в современном обществе

More than just information: The power of OSINT in modern society

Аннотация: В данной статье детально рассматривается Open Source Intelligence (OSINT) – стратегия сбора и анализа данных из открытых источников для достижения различных целей. Описаны методы OSINT, включая пассивные и активные подходы, а также выделены ключевые этапы процесса, включающие сбор, обработку, анализ информации, визуализацию результатов и отчетность. Также затрагивается разнообразие инструментов, используемых для эффективной реализации OSINT, рассмотрены перспективы развития этой области, с акцентом на интеграцию современных технологий.
Ключевые слова: OSINT, сбор, обработка, анализ, информационная безопасность, инструменты.
Abstract: This article discusses in detail Open Source Intelligence (OSINT), a strategy for collecting and analyzing data from open sources to achieve various goals. OSINT methods, including passive and active approaches, are described, and key stages of the process are highlighted, including the collection, processing, analysis of information, visualization of results and reporting. The variety of tools used for the effective implementation of OSINT is also touched upon, the prospects for the development of this area are considered, with an emphasis on the integration of modern technologies.
Key words: OSINT, collection, processing, analysis, information security, tools.

В современном цифровом мире, где данные играют ключевую роль, безопасность информации становится все более актуальной задачей. Одним из важных аспектов обеспечения информационной безопасности является использование открытых источников информации (OSINT).

OSINT расшифровывается как Open-source intelligence, разведка по открытым источникам. То есть сбор и анализ информации, полученной из разных общедоступных информационных каналов. По сути, такими источниками может быть что угодно: газеты и журналы, телевидение и радио, данные, публикуемые официальными организациями, научные исследования и доклады на конференциях и так далее [1].

Основная цель OSINT – предоставление достоверной, полезной и оперативной информации для принятия обоснованных стратегических и тактических решений в различных областях деятельности.

С использованием OSINT достигается раннее выявление потенциальных угроз, что становится ключевым элементом в обеспечении безопасности. Мониторинг общедоступных источников позволяет

оперативно реагировать на изменения в киберпространстве, такие как возможные атаки или утечки информации.

Однако OSINT выходит далеко за пределы простого выявления угроз. Эта технология играет важную роль в анализе репутации компаний и организаций. Сбор данных о деятельности в сети, отзывах клиентов и обсуждениях в социальных сетях позволяет выявить потенциальные угрозы репутации и предпринять меры по их предотвращению.

Еще одним важным аспектом применения OSINT является идентификация уязвимостей в инфраструктуре организации. Сбор данных из открытых источников позволяет выявлять возможные уязвимости, что в свою очередь способствует оперативному обеспечению безопасности и предотвращению возможных атак, основанных на известных уязвимостях.

Наконец, OSINT применяется для предотвращения социальной инженерии. Анализ информации, доступной в открытом доступе, позволяет выявлять возможные методы манипуляции и снижать риски финансовых мошенничеств и атак, основанных на обмане сотрудников.

В мире кибербразведки существует два основных метода сбора информации – пассивный и активный [2]. Каждый из них имеет свои особенности и применяется в зависимости от целей и контекста исследования.

1. Пассивный метод

В рамках пассивного метода сбора информации, исследователь воздействует на объект минимально, стремясь не оставлять цифрового следа. Собирая информацию, исследователь ограничивается использованием открытых источников, а также доступом к контенту, который объект исследования публично разместил. Это включает в себя анализ веб-сайтов, поиск архивной информации и использование методов, таких как анализ открытых баз данных, а также изучение публичных профилей в социальных сетях и мониторинг обсуждений на форумах.

2. Активный метод

В отличие от пассивного метода, активный метод подразумевает более прямое воздействие на объект исследования. Здесь исследователь активно взаимодействует с IT-инфраструктурой объекта, проводя сканирование сетей, анализ уязвимостей и даже применяя техники, которые могут быть замечены субъектом. Активные методы также включают социальную инженерию, где исследователь манипулирует людьми для получения ценной информации.

Каждый из этих методов имеет свои преимущества и ограничения. Пассивные методы обеспечивают низкую вероятность обнаружения, сохраняя анонимность и меньший шанс вызвать подозрение. В то время как активные методы могут предоставить более обширную информацию, они также повышают риск раскрытия исследователя. Искусное сочетание обоих

методов позволяет достичь баланса между полнотой собираемой информации и минимизацией рисков обнаружения.

Open Source Intelligence включает несколько этапов, в которые входит сбор, обработка и анализ информации. Эти этапы часто подразделяются следующим образом:

Сбор информации: Этот этап включает в себя активный и пассивный сбор данных из открытых источников. В зависимости от целей и задач, специалист по OSINT может использовать различные методы, такие как анализ веб-сайтов, мониторинг социальных сетей, изучение публичных документов и другие техники для сбора нужной информации.

Обработка данных: Полученные данные требуют обработки и структурирования для удобства анализа. В этот этап входит фильтрация, оценка достоверности и релевантности информации. Также может включать в себя преобразование данных в удобный формат для последующего анализа.

Анализ: На этом этапе специалисты проводят глубокий анализ данных с целью выявления закономерностей, тенденций, а также выделения ключевых факторов. Здесь может использоваться статистический анализ, методы машинного обучения и другие инструменты для извлечения значимой информации.

Визуализация результатов: Важной частью OSINT является представление данных в удобной форме. Это может включать в себя создание графиков, карт, диаграмм или других визуальных средств для лучшего понимания и интерпретации информации.

Отчетность: Результаты анализа представляются в виде отчета, который может быть использован для принятия решений, разработки стратегий или подготовки рекомендаций. Эффективная отчетность является ключевым элементом в успешной реализации OSINT.

Эти этапы OSINT формируют цикл процесса, обеспечивая эффективный и осведомленный анализ данных. Этот цикл является неотъемлемым элементом в различных областях, таких как информационная безопасность, разведка и бизнес-аналитика. Умение систематически собирать, обрабатывать, анализировать и визуализировать информацию из открытых источников становится критическим для принятия обоснованных решений, предотвращения угроз и выявления возможностей в разнообразных контекстах.

Для эффективного проведения разведки также используются различные средства и технологии. Это включает в себя специализированные программы для сбора и анализа данных, инструменты для мониторинга социальных сетей, а также методы открытого исследования веб-ресурсов. Рекомендуемые инструменты OSINT для исследования безопасности:

– Maltego – мощный графический инструмент для сбора и анализа данных. Этот программный продукт по заданным параметрам ищет

различную информацию по открытым (и не только открытым!) источникам. Он позволяет интегрировать информацию из различных источников и визуализировать ее в виде графа, что упрощает выявление связей между различными сущностями (людьми, организациями, доменами и т.д.). Maltego активно используется для проведения исследований на предмет потенциальных угроз и уязвимостей.

– Shodan – поисковая система для интернета вещей (IoT). Этот инструмент позволяет искать устройства, подключенные к ИТС «Интернет», и предоставляет информацию о них. С его помощью можно выявлять открытые порты, слабые места в системах безопасности, а также отслеживать изменения в структуре сетей.

– TheHarvester предназначен для сбора электронных адресов, поддоменов, хостов и другой информации из различных открытых источников, таких как поисковые системы, социальные сети, DNS-сервера и т.д. Этот инструмент часто используется для анализа поверхностного веб-пространства.

– SpiderFoot – автоматизированное средство OSINT с открытым исходным кодом, предназначенное для сбора данных о заданной цели. Оно объединяет информацию из различных источников, включая веб-страницы, базы данных, DNS-запросы и другие. SpiderFoot помогает в выявлении угроз, связанных с конкретными сущностями.

– OSINT Framework представляет собой набор различных инструментов и ресурсов, собранных в одном месте для облегчения исследований в области открытых источников. Этот фреймворк включает в себя ссылки на различные инструменты и ресурсы для сбора информации. Не рассчитан для применения в России.

– FOCA (Fingerprinting Organizations with Collected Archives) – инструмент для анализа документов Microsoft Office и других файлов, с целью извлечения скрытой метаинформации, которая может быть полезна для выявления сущностей и их связей.

– Google Dorks – это строка поиска, используемая для выявления конкретных уязвимостей и утечек информации через поисковую систему Google. Эти специальные запросы позволяют исследователям проводить более точный и тщательный поиск в открытых источниках. Аргументы операторов поиска позволяют обрабатывать запросы практически любого типа данных (в том числе имена пользователей и пароли).

– SOCMINT (Social Media Intelligence) инструменты, такие как Echosec и Creepy, позволяют анализировать информацию из социальных сетей. Они могут быть использованы для выявления угроз, анализа общественного мнения и мониторинга активности в цифровом пространстве.

Эти инструменты предоставляют исследователям и специалистам по безопасности мощные средства для эффективного мониторинга, анализа репутации, выявления уязвимостей и других задач. Важно отметить, что разнообразие инструментов позволяет адаптировать подход к конкретным целям и контекстам, обеспечивая точный и информированный анализ в различных областях, таких как кибербезопасность, бизнес-аналитика и разведка. Однако необходимо также учитывать этические аспекты при использовании подобных инструментов, чтобы обеспечивать соблюдение законов и принципов конфиденциальности.

Использование OSINT в информационной безопасности становится все более важным компонентом стратегии защиты данных. Этот подход позволяет предотвращать угрозы на ранних стадиях, анализировать репутацию, выявлять уязвимости и снижать риски социальной инженерии. Развитие средств и технологий OSINT продолжит играть ключевую роль в создании устойчивой и надежной информационной безопасности.

В будущем OSINT будет развиваться в направлении большей автоматизации и точности с помощью искусственного интеллекта и машинного обучения. Также возможно расширение области применения OSINT на такие сферы, как анализ больших данных и обработка естественного языка.

Заключение. В современном цифровом мире, где информация играет ключевую роль, открытые источники информации (OSINT) становятся незаменимым инструментом для обеспечения информационной безопасности. OSINT позволяет выявлять потенциальные угрозы, оценивать репутационные риски и обнаруживать уязвимости, используя как пассивные, так и активные методы сбора данных.

Применение специализированных инструментов и технологий, включая искусственный интеллект и машинное обучение, делает OSINT еще более мощным и эффективным. Развитие OSINT и его интеграция в стратегии информационной безопасности позволяет компаниям повысить ситуационную осведомленность и своевременно реагировать на потенциальные угрозы.

Таким образом, OSINT играет важную роль в современных стратегиях кибербезопасности, и его значение будет только увеличиваться по мере развития технологий и роста объемов доступных открытых данных.

Библиографический список:

1. Kaspersky daily | Блог Касперского: Что такое OSINT и в чем опасность [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/osint-open source-intelligence/35955/ (Дата обращения: 05.01.2024)

2. Навыки OSINT(интернет-разведки) в кибербезопасности: [Электронный ресурс]. URL: https://proglib-io.turbopages.org/proglib.io/s/p/navyki-osint-internet-razvedki-v-kiberbezopasnosti-2020-11-14 (Дата обращения: 05.01.2024)
3. OSINT или разведка по открытым источникам: [Электронный ресурс]. URL: https://habr.com/ru/companies/deiteriylab/articles/595801/ (Дата обращения: 05.01.2024)
4. 8+4 инструмента OSINT: как обойти ваших конкурентов и не стать жертвой: [Электронный ресурс]. URL: https://vc.ru/marketing/926676-8-4-instrumenta-osint-kak-oboyti-vashih-konkurentov-i-ne-stat-zhertvoy (Дата обращения: 05.01.2024)
5. Как использовать Maltego для OSINT: практическое руководство [Электронный ресурс]. https://www.securitylab.ru/blog/personal/SimlpeHacker/353048.php?ysclid=lrm7q0tyi223873805 (Дата обращения: 05.01.2024)
6. Shodan – темный близнец Google: [Электронный ресурс]. https://habr.com/ru/companies/ruvds/articles/517638/ (Дата обращения: 05.01.2024)

УДК 004.056

Степанов Максим Олегович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Нагаев Назим Харисович, научный руководитель, старший преподаватель кафедры «Системы информационной безопасности»
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, Student
Lukyanov Emil Radikovich, Student
Misbachov Niaz Ilyasovich, Student
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI

Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer of the department "Si" "Information security system"
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI
Russland, Kasan

Использование технологии блокчейн в кибербезопасности

The use of blockchain technology in cybersecurity

Аннотация: В данной статье рассматривается применение технологии блокчейн в области безопасности. В тексте описывается принцип работы технологии, основанный на использовании хеш-сумм. Также приводятся такие примеры использования блокчейн-технологии в сфере кибербезопасности, как защита личных данных в социальных сетях, обеспечение безопасности передачи данных, противодействие атакам DDoS, использование блокчейна в инфраструктуре открытых ключей и обеспечение целостности программного обеспечения. Несмотря на свой значительный потенциал для укрепления кибербезопасности, подчеркиваются также недостатки технологии блокчейн, которые следует учитывать.
Ключевые слова: блокчейн, технология, хеш, безопасность, защита данных.
Abstract: This article discusses the application of blockchain technology in the field of security. The text describes the principle of operation of the technology based on the use of hash sums. There are also examples of the use of blockchain technology in the field of cybersecurity, such as protecting personal data on social networks, ensuring data transfer security, countering DDoS attacks, using blockchain in public key infrastructure and ensuring software integrity. Despite its significant potential to strengthen cybersecurity, the disadvantages of blockchain technology are also highlighted, which should be taken into account.
Key words: blockchain, technology, hash, security, data protection.

В эпоху активного развития цифровых технологий, когда масштабные технологические инновации сменяют друг друга с поразительной скоростью, вопросы кибербезопасности становятся все более актуальными и насущными. С увеличением числа цифровых атак, киберпреступников и угроз, необходимость в эффективных методах защиты данных и информационных ресурсах становится критической. В этом контексте технология блокчейн выступает в роли инновационного и перспективного инструмента, который изменяет представление о привычных подходах к обеспечению кибербезопасности.

Блокчейн (англ. blockchain, изначально block chain – цепь из блоков) – выстроенная по определенным правилам непрерывная последовательная цепочка блоков (связный список), содержащих какую-либо информацию [1].

Важной особенностью блокчейна является обеспечение связи между блоками не только за счет нумерации, но и благодаря применению хеш-сумм. Каждый блок несет в себе не только свою уникальную хеш-сумму, но и хеш-сумму предыдущего блока. Любое изменение внесенной информации в блок приводит к изменению его хеш-суммы. Для соблюдения правил построения цепочки блоков, такие изменения необходимо отразить в следующем блоке, что также вызовет пересчет хеш-суммы в этом блоке. Этот механизм гарантирует, что изменения в одном блоке сразу заметны и влияют на все последующие блоки. Схема показана рисунке 1.

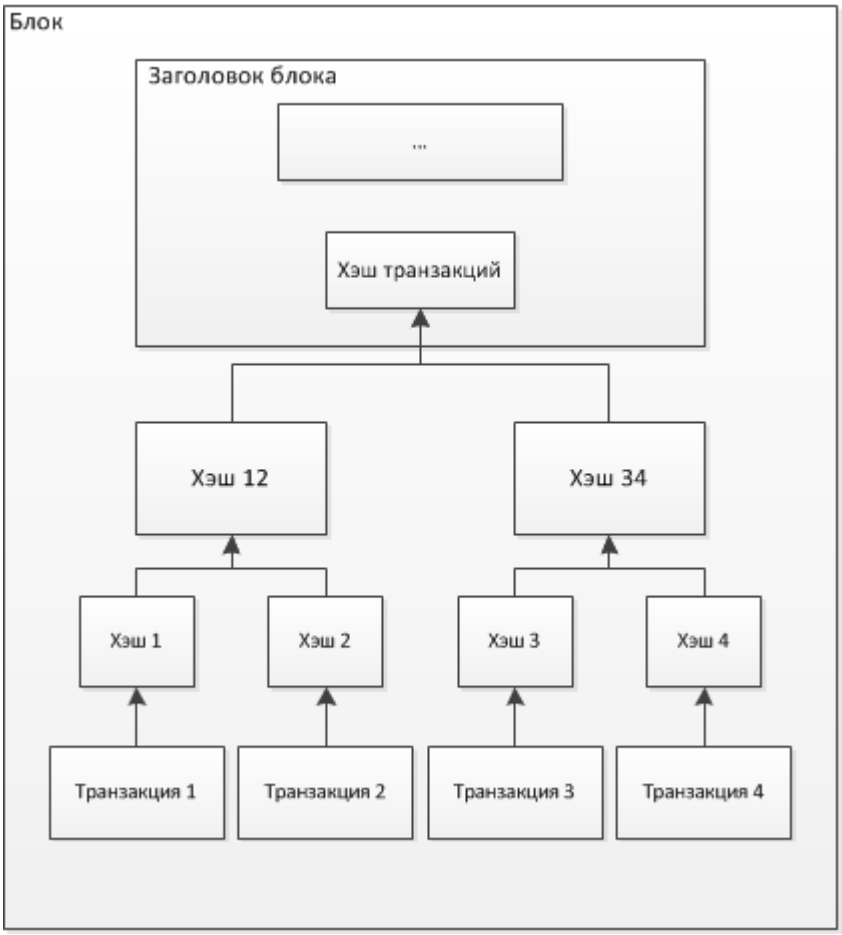


Рис.1. Схема получения хеша транзакций

Кроме того, благодаря децентрализованному хранению копий цепочек блоков на множестве независимых компьютеров, блокчейн обеспечивает высокий уровень устойчивости и надежности. Эта технология открывает перед собой перспективы для создания безопасных, прозрачных и устойчивых систем, где манипуляции данными практически исключены, а цифровые активы и транзакции поддерживаются с высоким уровнем доверия и эффективности.

Примеры использования блокчейна в кибербезопасности:

1. Защита социальных сетей

В современном мире, где социальные сети становятся главным средством общения, защита личной информации становится ключевой задачей. В условиях роста популярности социальных приложений и увеличения количества пользователей, безопасность обмена сообщениями становится особенно важной. Многие пользователи, однако, используют слабые пароли, оставляя свою личную информацию под угрозой. Многие компании в сфере обмена сообщениями и социальных сетей обращают внимание на блокчейн в качестве эффективного средства защиты данных. Он предоставляет превосходное решение для сквозного шифрования, которое может быть более надежным, чем многие существующие методы. Блокчейн может служить основой для стандартного протокола безопасности, улучшая способы защиты данных пользователей.

Недавние атаки на социальные сети, такие как Twitter и Facebook, подчеркивают неотложность проблемы. В 2020 году, атаки хакеров на аккаунты известных личностей в Twitter позволили злоумышленникам размещать мошеннические сообщения, обманывая подписчиков. Эти инциденты привлекли внимание к вопросам безопасности в социальных медиа [2].

Благодаря использованию блокчейна можно усовершенствовать защиту личных данных пользователей и внедрить более надежные методы проверки подлинности, обеспечивая повышенный уровень безопасности.

2. Защита передачи данных с помощью блокчейна

Блокчейн предоставляет перспективное решение для предотвращения несанкционированного доступа к данным в процессе их передачи. Путем применения механизма полного шифрования блокчейн обеспечивает защиту передаваемых данных, тем самым мешая злоумышленникам. Этот подход стремится к повышению общего уровня доверия и целостности данных, передаваемых через блокчейн. В существующих каналах связи, таких как электронная почта, хакеры с зловредными намерениями могут подключаться к данным в процессе передачи, внося изменения или даже полностью удаляя их. Использование блокчейна создает барьер, препятствуя подобным атакам, тем самым поднимая уровень эффективности и безопасности в процессе обмена информацией.

3. Борьба с DDoS

Технология блокчейн активно используется в борьбе с DDoS-атаками. Децентрализация данных делает систему менее уязвимой перед массовыми атаками, распределение информации по сети усложняет задачу хакерам. Консенсусные механизмы, такие как Proof-of-Work, это алгоритм консенсуса, используемый для достижения соглашения, который определяет, какие из блоков будут добавлены в цепочку после майнинга, и Proof-of-Stake, это категория согласованных алгоритмов для открытых цепочек блоков, которые зависят от экономических интересов валидатора в сети, повышают уровень

защиты [3]. Блокчейн позволяет создавать смарт-контракты, это компьютерный алгоритм, предназначенный для формирования, управления и предоставления информации о владении чем-либо, для точного управления трафиком и эффективной фильтрации подозрительных запросов [4].

«Умные смарт-контракты» анализируют паттерны трафика, обнаруживая аномалии. Применение криптографии обеспечивает дополнительный уровень безопасности. Благодаря отсутствию единой точки отказа, блокчейн устойчив к DDoS-атакам, обеспечивая надежность всей сетевой инфраструктуры.

4. Использование блокчейна в инфраструктуре открытых ключей (PKI)

Блокчейн может быть использован для хранения, управления и верификации цифровых сертификатов, которые играют ключевую роль в процессе аутентификации. Блокчейн обеспечивает децентрализованное хранение цифровых сертификатов, их неизменяемость и прозрачность. Ведь каждый блок в цепи блокчейна содержит хеш предыдущего блока и свою хеш-сумму, обеспечивая неизменяемость истории изменений. Это гарантирует, что информация о сертификатах остается неподдельной, а вся история доступна для проверки [5].

5. Усиление безопасности DNS

Система доменных имен (DNS), подобная общедоступному каталогу, связывающему доменные имена с IP-адресами, подвержена атакам хакеров. Неизменяемость и децентрализованные системы блокчейна обеспечивают повышенный уровень безопасности хранения записей DNS. Такой подход снижает риск несанкционированного доступа, защищая DNS от потенциальных атак, которые могут поставить под угрозу доступность веб-сайта [5].

6. Обеспечение целостности программного обеспечения

Блокчейн-технология позволяет осуществлять проверку целостности загружаемого и устанавливаемого программного обеспечения, обеспечивая надежную защиту от вредоносных атак.

Идея заключается в том, что хеши, представляющие уникальные идентификаторы программного обеспечения, регистрируются в блокчейне. Это формирует надежный реестр, который может быть использован для сопоставления с новыми идентификаторами программного обеспечения. Такой метод обеспечивает эффективную проверку подлинности загрузок и обновлений, что, в свою очередь, защищает устройства от возможных нарушений безопасности.

Таким образом, технология блокчейн может значительно улучшить кибербезопасность, обеспечивая безопасность данных и создавая надежные системы обмена информацией. Однако у данной технологии есть ряд недостатков:

– Процесс майнинга и поддержания блокчейна требует значительных вычислительных ресурсов, что может привести к экологическим и энергетическим проблемам.

– Некоторые блокчейн-сети сталкиваются с ограничениями в масштабируемости, что затрудняет их применение в крупных системах с высокой производительностью.

– Внедрение блокчейна в существующие системы может быть сложным процессом, требующим изменений в бизнес-процессах и обучении персонала.

– Отсутствие четкого законодательства и регулирования в области блокчейна может создавать правовые сложности и вызывать неопределенность в области кибербезопасности.

– Смарт-контракты, работающие на блокчейне, могут содержать ошибки или уязвимости, которые могут быть использованы злоумышленниками.

– Безопасность блокчейна может зависеть от деятельности участников сети. Если большинство вычислительной мощности контролируется злоумышленниками, это может угрожать целостности системы.

– Блокчейн в значительной степени полагается на закрытые ключи для шифрования данных, а невосстановимость утерянных закрытых ключей создает риск постоянной недоступности данных.

– Несмотря на множество применений блокчейна в сфере кибербезопасности, существует нехватка квалифицированных разработчиков, требующих глубоких знаний различных инструментов разработки и языков программирования. Этот дефицит препятствует широкому внедрению технологии блокчейн в практику кибербезопасности.

Заключение. Технология блокчейн представляет собой перспективный инструмент, способный внести значительный вклад в обеспечение кибербезопасности. Ее уникальные особенности, такие как прозрачность, безопасность и отслеживаемость, делают ее идеальным инструментом для защиты данных и создания безопасных сетей. Кроме того, она может снизить риск мошенничества благодаря использованию криптографии для защиты информации. В настоящее время многие компании и организации активно изучают возможности применения блокчейн в своих системах для повышения уровня безопасности. С развитием технологии и ростом интереса, можно ожидать еще более широкого использования в будущем.

Библиографический список:

1. Блокчейн: [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD (Дата обращения: 06.01.2024)
2. Массовый взлом Twitter. Как хакерам это удалось и сколько они заработали: [Электронный ресурс]. URL: https://hightech.fm/2020/07/16/hackers-twitter (Дата обращения: 06.01.2024)
3. Безопасность, децентрализация и равные права. Как работает блокчейн: [Электронный ресурс]. URL: https://www.rbc.ru/crypto/news/5fe6f4d99a794739760fe17f?from=copy (Дата обращения: 06.01.2024)
4. Смарт-контракт: [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82-%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%B0%D0%BA%D1%82 (Дата обращения: 06.01.2024)
5. Blockchain Based DNS and PKI Solutions: [Электронный ресурс]. URL: https://e-tarjome.com/storage/btn_uploaded/2022-08-02/1659417394_12473-English.pdf (Дата обращения: 06.01.2024)

УДК 004.056

Степанов Максим Олегович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Нагаев Назим Харисович, научный руководитель, старший преподаватель кафедры «Системы информационной безопасности»
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, Student
Lukyanov Emil Radikovich, Student
Misbachov Niaz Ilyasovich, Student
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI
Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer of the department "Si" "Information security system"
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI
Russland, Kasan

Исследование уязвимости Path Traversal

Investigating the vulnerability of Path Traversal

Аннотация: В данной статье рассматривается одна из наиболее опасных уязвимостей веб-приложений - уязвимость Path Traversal. В тексте исследуются причины возникновения этой уязвимости, методы ее эксплуатации и предлагаются эффективные стратегии защиты от атак. Рассматривается конкретная уязвимость CVE-2021-41773 в HTTP-сервере Apache, а также разобран наиболее частый способ эксплуатации этой

уязвимости. В статье представлены практические советы и методы защиты, такие как фильтрация пользовательского ввода, применение абсолютных путей, ограничение прав доступа, а также настоятельное рекомендация по регулярному обновлению системы и приложений для поддержания безопасности на должном уровне.
Ключевые слова: уязвимость обхода пути, Path Traversal, веб-приложение, информационная безопасность.
Abstract: This article discusses one of the most dangerous vulnerabilities of web applications - the Path Traversal vulnerability. The text explores the causes of this vulnerability, the methods of its exploitation and suggests effective strategies to protect against attacks. The specific vulnerability CVE-2021-41773 in the Apache HTTP server is considered, and the most common way of exploiting this vulnerability is also analyzed. The article provides practical tips and protection methods, such as filtering user input, using absolute paths, restricting access rights, as well as an urgent recommendation for regular updates of the system and applications to maintain security at the proper level.
Key words: vulnerability of path traversal, Path Traversal, web application, information security.

Уязвимость обхода пути (Path Traversal) - это злонамеренная попытка заставить веб-приложение отобразить содержимое каталога, отличного от того, который запрошен пользователем, и получить доступ к конфиденциальным файлам на сервере [1]. Это достигается путем указания пути к файлу, находящемуся за пределами ожидаемого каталога, или путем использования специальных символов, которые позволяют злоумышленнику перемещаться по файловой системе.

Эта уязвимость является общей проблемой в веб-приложениях, часто вызванной недостаточным контролем и фильтрацией входных данных. Когда злоумышленник способен эксплуатировать уязвимость обхода пути, он может получить доступ к информации, которая в обычных условиях должна быть недоступна. Это может включать в себя конфигурационные файлы, персональные данные или даже сервер в целом. Уязвимость обхода пути также может быть использована для запуска произвольного кода на сервере, что может привести к полному нарушению безопасности системы.

В области информационной безопасности существует база данных со всеми общеизвестными уязвимостями, под названием CVE (Common Vulnerabilities and Exposures). Каждая уязвимость, зарегистрированная в системе CVE, имеет уникальный идентификатор, который облегчает отслеживание и обмен информацией о безопасности между организациями и специалистами по информационной безопасности [2].

CVE-2021-41773 - это конкретный идентификатор уязвимости, связанный с уязвимостью обхода пути в HTTP-сервере Apache, которая

позволяет злоумышленнику сопоставлять URL-адреса с файлами за пределами ожидаемого корня документа. Это означает, что злоумышленник может использовать специально сформированные URL-адреса для обхода ограничений доступа к файлам и каталогам на сервере Apache [3].

Пример использования уязвимости обхода пути в CVE-2021-41773 может быть следующим: злоумышленник может сконструировать URL-адрес таким образом, чтобы обмануть HTTP-сервер Apache и получить доступ к файлам, на которые не должен иметь доступа. Это может позволить злоумышленнику просматривать, изменять или удалять конфиденциальные файлы на сервере, что представляет серьезную угрозу для безопасности данных и инфраструктуры.

При наиболее частом способе эксплуатации уязвимости Path Traversal злоумышленник может использовать различные HTTP-методы, такие как GET, POST, PUT и другие, для осуществления атаки обхода пути на уязвимом веб-сайте. В типичном сценарии атаки [4]:

– Пользователь обращается к динамическому URL-адресу уязвимого сайта,
например, https://vulnerablewebsite.com/show.asp?view=homepage.html.

– Сервер получает запрос на страницу show.asp с параметром view=homepage.html и отправляет необходимую страницу, написанную на show.asp.

– Злоумышленник обнаруживает, что страница show.asp позволяет получить доступ к любому файлу, указанному в параметре view URL-адреса.

– Злоумышленник создает специально сформированный URL-адрес с относительным путем, используя символы "../", например, https://www.vulnerablewebsite.com/download_file.php?file=../../etc/passwd, или с абсолютным путем, например, http://vulnerablewebsite/get.asp?f=/etc/passwd, который запрашивает файл /etc/passwd.

– Поскольку уязвимый сервер не проверяет вводимые пользователем данные, злоумышленник может выйти из корневого каталога сети и получить доступ к вашим системным файлам; в данном случае файл passwd.

В результате недостаточной проверки вводимых данных сервером, злоумышленник может успешно выполнить атаку Path Traversal, что представляет серьезную угрозу для безопасности данных и инфраструктуры сервера.

Предотвращение атак с обходом пути критически важно для обеспечения безопасности веб-приложений. Рассмотрим несколько методов, которые помогут защитить систему от этого типа атак:

– Фильтрация пользовательского ввода: Один из наиболее важных способов предотвращения атак с обходом пути - это тщательная фильтрация и валидация пользовательского ввода. Необходимо убедиться, что все пользовательские данные, особенно те, которые могут быть использованы для формирования путей к файлам или директориям, проходят строгую проверку на наличие недопустимых символов или конструкций.

– Использование абсолютных путей: Вместо использования относительных путей к файлам и директориям рекомендуется использовать абсолютные пути. Это поможет избежать возможности навигации по файловой системе сервера и ограничит доступ к конфиденциальным данным.

– Ограничение прав доступа: Необходимо гарантировать, что файлы и директории на сервере имеют минимально необходимые права доступа. Это поможет ограничить возможные угрозы в случае успешной атаки с обходом пути, предотвратив несанкционированный доступ к конфиденциальным данным.

– Использование белого списка: Создание белого списка позволяет разрешить доступ только к тем файлам и директориям, которые являются известными и безопасными. При обработке запросов к ресурсам на сервере необходимо проверять, соответствуют ли запрашиваемые файлы и директории списку допустимых ресурсов. Если ресурс не находится в белом списке, доступ к нему должен быть запрещен.

– Использование "песочницы": Следует ограничить доступ к файловой системе так, чтобы злоумышленники не могли получить доступ к конфиденциальным файлам и директориям. Это можно сделать с помощью настройки прав доступа к файлам и директориям на уровне операционной системы.

– Обновление системы и приложений: Необходимо регулярно обновлять операционную систему, веб-сервер, сервер приложений и другое программное обеспечение с целью устранения известных уязвимостей, которые могут быть использованы для атак Path Traversal.

Применение этих методов поможет укрепить защиту системы от атак с обходом пути и снизить риск компрометации конфиденциальных данных.

Заключение. Уязвимость Path Traversal представляет серьезную угрозу для безопасности веб-приложений и серверов, так как злоумышленники могут использовать её для доступа к конфиденциальным данным и выполнения вредоносных действий. В случае успешной атаки с обходом пути, злоумышленники получают доступ к файлам и директориям, на которые не должны иметь доступа, что приводит к утечке информации и нарушению целостности системы.

Обеспечение безопасности данных и инфраструктуры является первостепенной задачей при разработке и поддержке веб-приложений. Постоянное обновление знаний и методов защиты от уязвимостей не только сохраняет целостность и конфиденциальность данных, но и обеспечивает надежность системы в цифровой среде. Следование рекомендуемым стандартам безопасности помогает сократить риски нарушения безопасности и обеспечивает надежную защиту от возможных угроз.

Библиографический список:

1. What is Path Traversal: [Электронный ресурс]. URL: https://www.stackhawk.com/blog/what-is-path-traversal/ (Дата обращения: 21.02.2024))
2. Common Vulnerabilities and Exposures: [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures (Дата обращения: 21.02.2024)
3. How To Fix CVE-2021-41773 A Path Traversal And File Disclosure Vulnerability In Apache?: [Электронный ресурс]. URL: https://thesecmaster.com/how-to-fix-cve-2021-41773-a-path-traversal-and-file-disclosure-vulnerability-in-apache/ (Дата обращения: 21.02.2024)
4. What are path traversal attacks and how can you defend against them?: [Электронный ресурс]. URL: https://www.comparitech.com/blog/information-security/path-traversal-attacks/ (Дата обращения: 21.02.2024)

УДК 004.056

Степанов Максим Олегович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Нагаев Назим Харисович, научный руководитель, старший преподаватель кафедры «Системы информационной безопасности»
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, Student
Lukyanov Emil Radikovich, Student
Misbachov Niaz Ilyasovich, Student
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI
Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer of the department "Si" "Information security system"
Kasaner Nationale Israelische Technische Universität namens A.N. Tupolev-KAI
Russland, Kasan

Социальная инженерия: методы атак и способы предотвращения

Social engineering: methods of attacks and ways of prevention

Аннотация: В данной статье исследуется понятие социальной инженерии и ее роль в современной информационной безопасности. Рассматриваются

различные методы социальной инженерии, используемые злоумышленниками для манипуляции и обмана людей с целью получения конфиденциальной информации или доступа к системам. Особое внимание уделяется способам предотвращения атак, использующих социальную инженерию. Предлагаются практические рекомендации, которые могут быть использованы организациями и пользователями для защиты от таких атак.
Ключевые слова: социальная инженерия, атаки, предотвращение, информационная безопасность.
Abstract: This article explores the concept of social engineering and its role in modern information security. Various methods of social engineering used by attackers to manipulate and deceive people in order to obtain confidential information or access systems are considered. Special attention is paid to ways to prevent attacks using social engineering. Practical recommendations are offered that can be used by organizations and users to protect against such attacks.
Key words: social engineering, attacks, prevention, information security.

В современном информационном обществе, где цифровые технологии проникают во все сферы нашей жизни, безопасность и конфиденциальность становятся все более актуальными вопросами. Однако, несмотря на развитие современных систем защиты, злоумышленники находят новые способы обхода этих мер и получения доступа к конфиденциальной информации. Один из таких способов – социальная инженерия.

Социальная инженерия – это совокупность подходов прикладных социальных наук, приемов и технологий, ориентированных на создание организационных структур для регулирования и управления действиями человека [1].

Социальная инженерия является очень опасным методом атаки, поскольку она напрямую зависит от человеческого фактора. Злоумышленники используют психологические манипуляции и обман, чтобы убедить людей раскрыть конфиденциальную информацию или выполнить определенные действия, которые могут привести к утечке данных, финансовым потерям или нарушению безопасности.

Существует множество методов социальной инженерии, которые злоумышленники могут использовать для достижения своих целей. Рассмотрим некоторые из них:

1. Фишинг (от англ. fishing – рыбалка)

Фишинг – вид интернет-мошенничества, цель которого является получение идентификационных данных пользователей [6].

Фишинговые атаки являются формой мошенничества, при которой злоумышленники используют электронные коммуникации для обмана пользователей и получения их конфиденциальной информации или распространения вредоносных программ. Чаще всего фишинговые атаки

направлены на получение логинов, паролей, данных кредитных карт и других личных данных.

Фишинг может осуществляться различными способами. Один из распространенных методов – это отправка электронных писем, которые выглядят подлинными и призывают пользователей ввести свои личные данные на поддельных веб-сайтах. Жертвы, не подозревая об обмане, могут предоставить свои данные злоумышленникам.

Кроме того, фишинговые атаки могут использовать другие механизмы для нанесения вреда. Например, после перехода на поддельный сайт жертва может столкнуться с установкой вредоносного шпионского ПО на свой компьютер или с атакой программы-вымогателя, которая может зашифровать данные на компьютере и требовать выкуп для их восстановления. Также возможны атаки на компании, где фишинговые электронные письма отправляются для получения регистрационной информации сотрудников или других данных, которые могут быть использованы для дальнейших атак на компанию.

2. Baiting (от англ. baiting – приманка)

Этот метод социальной инженерии использует человеческое любопытство как слабое звено в цепи безопасности. Злоумышленники оставляют зараженные устройства в местах, где их легко найти, или предлагают заманчивые предложения в Интернете, которые приводят к зараженным сайтам или загрузке вредоносного ПО.

Важно отметить, что приманки могут быть очень разнообразными, и злоумышленники постоянно усовершенствуют свои методы. Это может включать все, от физических устройств, таких как USB-накопители или CD-диски, до цифровых "подарков", таких как бесплатные приложения, игры, музыка или фильмы. В любом случае, целью является убедить потенциальную жертву взаимодействовать с зараженным содержимым.

3. Кви про кво (от англ. quid pro quo – услуга за услугу)

Кви про кво представляет собой метод социальной инженерии, который включает в себя использование голосовой связи для проведения атак. В данном сценарии злоумышленник звонит по случайному номеру в организацию, притворяясь сотрудником технической поддержки или представителем другого доверенного сервиса.

Атака обычно начинается с того, что злоумышленник информирует жертву о возможных технических проблемах и предлагает ей помощь в их решении. В процессе такого общения атакующий может попросить жертву предоставить конфиденциальные данные или даже ввести определенные команды, эти действия приводят к запуску вредоносного ПО или же к краже регистрационных данных.

4. Претекстинг (от англ. pretext – повод, предлог)

Претекстинг – это мошенническая схема, основанная на методах социальной инженерии. Целью злоумышленника является получение конфиденциальных данных. Чаще всего преступники охотятся за финансовой информацией – паролем и логином от онлайн-банка, PIN-кодом кредитной карты и т.п [6].

Претекстинг представляет собой форму социальной инженерии, при которой злоумышленник выдаёт себя за другого человека с целью получения конфиденциальной информации. Злоумышленник может представляться другим человеком, например, сотрудником компании, представителем банка или другой доверенной организации. Этот вид атаки требует тщательной подготовки со стороны злоумышленника, включая сбор и использование заранее изученной информации, такой как день рождения, ИНН, номер паспорта или последние цифры счета. Важной характеристикой претекстинга является создание убедительной истории, чтобы создать иллюзию подлинности и доверия.

5. Троянский конь

Троянский конь – вид вредоносной программы. Компьютерные трояны содержат в себе разрушительную нагрузку. Вложения электронной почты, содержащие скрытые вредоносные программы, являются формой трояна. Хитрость социальной инженерии заключается в том, что электронная почта, с которой отправляется вредоносный файл, исходит от надежного отправителя (коллега, друг, член семьи или компании, с которой человек ведет бизнес) [8].

Эти вредоносные программы внешне выглядят как легальный программный продукт, но при запуске осуществляют несанкционированные пользователем действия, направленные на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей [2].

6. Плечевой серфинг

Основывается на невнимательности жертвы, которая уверена в своей безопасности и никак не защищает конфиденциальные данные. Злоумышленник осуществляет контакт в общественном месте с жертвой и свободно подсматривает информацию, которая находится в открытом доступе на экранах мобильных устройств [9].

7. Фарминг

Фарминг – это разновидность фишинга, который состоит в изменении DNS-адреса так, чтобы веб-страницы, которые посещает пользователь, были не оригинальными, а другими, специально созданными злоумышленниками для сбора конфиденциальной информации, особенно такой, которая относится к онлайновым банкам [2].

Фарминг – вид кибератаки, целью которой является скрытное перенаправление пользователя на принадлежащий злоумышленнику фишинговый ресурс [6].

Это процедура скрытного перенаправления жертвы на ложный IP-адрес. Для этого может использоваться навигационная структура (файл hosts, система доменных имен (DNS)). Злоумышленник распространяет на компьютеры пользователей специальные вредоносные программы, которые после запуска на компьютере перенаправляют обращения к заданным сайтам на поддельные сайты. Обеспечивается высокая скрытность атаки, главное дождаться, когда пользователь решит посетить интересующие злоумышленника сайты. Вредоносные программы, реализующие фарминг атаку, используют два основных приема для скрытного перенаправления на поддельные сайты – манипулирование файлом HOSTS или изменением информации DNS.

8. Вишинг

Вишинг – метод социальной инженерии, разновидность фишинга, при котором злоумышленники используют голосовую связь, обманывая людей и заставляя их раскрывать конфиденциальную информацию. Злоумышленники могут подделывать номера телефонов, чтобы они выглядели как официальные, доверенные источники. Они могут притворяться сотрудниками банков, представителями компаний или даже государственными органами. Например, злоумышленник может позвонить, представившись сотрудником банка, и уведомить жертву о подозрительной активности на ее счете. Чтобы "помочь" в расследовании, злоумышленник может запросить подтверждение личных данных, таких как номера счетов, пин-коды и другие сведения.

Проанализированы основные методы социальной инженерии, используемые злоумышленниками для манипуляции человеческим фактором в целях получения конфиденциальной информации. Однако важно отметить, что существует множество разнообразных методов, и их количество постоянно растет вместе с развитием технологий.

Важно понимать, что полностью избежать социальной инженерии невозможно. Однако существуют меры, которые помогают снизить риски и уменьшить уязвимость к подобным атакам.

Рассмотрим несколько способов противодействия социальной инженерии:

– Обучение и осведомленность: Один из самых эффективных способов борьбы с социальной инженерией – это обучение сотрудников и повышение их осведомленности о методах атак. Регулярные тренинги и обучающие программы помогут сотрудникам распознавать подозрительные ситуации и быть более бдительными.

– Проверка источников: Важно проверять источник звонков, электронных писем и ссылок, прежде чем предоставлять конфиденциальную информацию или выполнять какие-либо действия. Не следует доверять непроверенным источникам, необходимо проявлять осторожность при взаимодействии с неизвестными лицами.

– Сильные пароли и многофакторная аутентификация: Пользователям необходимо использовать сложные пароли и регулярно их менять. Для дополнительного уровня защиты рекомендуется включить многофакторную аутентификацию.

– Ограничение доступа к конфиденциальной информации: Доступ к конфиденциальной информации необходимо предоставлять только сотрудникам, имеющим право доступа к данной информации. Установить строгие политики безопасности и контроль доступа.

– Регулярное обновление программного обеспечения: Необходимо регулярно обновлять операционные системы, приложения и антивирусное программное обеспечение, чтобы устранить уязвимости и защититься от известных угроз.

– Внимательность к деталям: Важно быть внимательным к деталям при получении электронных писем, посещении веб-страниц и получении запросов на информацию. Рекомендуется обращать внимание на грамматические ошибки, странные ссылки или неожиданные запросы на информацию.

– Частые резервные копии данных: Создание резервных копий данных и их безопасное хранение помогут восстановить информацию в случае атаки, утечки данных, а также при случайной потере или повреждении файлов. Это важная мера безопасности, которая поможет защитить данные и обеспечить их доступность в случае необходимости.

– Политики безопасности: Необходимо установить строгие корпоративные политики безопасности, которые должны включать правила по обработке конфиденциальной информации, общение сотрудников с посторонними лицами и процедуры реагирования на инциденты.

Все эти меры помогут укрепить безопасность и повысить осведомленность сотрудников о социальной инженерии. Однако важно помнить, что безопасность является непрерывным процессом, и регулярное обновление и адаптация мер безопасности являются неотъемлемой частью защиты от новых угроз.

Эффективное противодействие социальной инженерии требует комплексного подхода, включающего в себя как организационные, так и технические меры безопасности. С учетом динамичности киберугроз и постоянного развития новых методов, построение безопасности и постоянное

обучение персонала остаются ключевыми компонентами в обеспечении информационной безопасности.

Заключение. Социальная инженерия представляет серьезную угрозу, поскольку использует уязвимость человеческого фактора. Несмотря на прогресс технологий, люди по-прежнему остаются наиболее слабым звеном защиты информации. Это подчеркивает важность сбалансированного подхода, уделяющего внимание как техническим, так и организационным мерам. В частности, необходимо обучать пользователей методам распознавания социальной инженерии и формировать культуру безопасного поведения в сети. Только комплексные меры, учитывающие как технологические, так и человеческий аспекты, могут эффективно противостоять этой значимой киберугрозе.

Библиографический список:

5. Митник, К.Д. Искусство обмана / К.Д. Митник, В.Л. Саймон // Компания АйТи. – 2004. – 360 с. (Дата обращения: 08.01.2024)

6. Нагаев, Н.Х. Антивирусная безопасность цифровой информации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2023. – 212 с.: ил.

7. Phishing attacks: [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/phishing-attack-scam/ (Дата обращения: 08.01.2024)

8. Cybersecurity Deep Dive: What Is a Baiting Attack?: [Электронный ресурс]. URL: https://www.privacyaffairs.com/what-is-a-baiting-attack/ (Дата обращения: 08.01.2024)

9. Quid pro quo social engineering: [Электронный ресурс]. URL: https://legal.thomsonreuters.com/blog/quid-pro-quo-social-engineering-infographic-and-explanation/ (Дата обращения: 08.01.2024)

10. Вирусная энциклопедия «Касперского». [Электронный ресурс]. (дата обращения 08.01.2024 г.) – URL: https://encyclopedia.kaspersky.ru/.

11. Kaspersky daily | Блог Касперского: Приёмы социальной инженерии [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/social-engineering-tricks/35654/ (Дата обращения: 08.01.2024)

12. Янгаева М.О. Методы (техники) социальной инженерии, используемые при совершении преступлений в сфере компьютерной информации: [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/metody-tehniki-sotsialnoy-inzhenerii-ispolzuemye-pri-sovershenii-prestupleniy-v-sfere-kompyuternoy-informatsii/viewer (Дата обращения: 08.01.2024)

13. Социальная инженерия: [Электронный ресурс]. URL: https://rt-solar.ru/products/solar_dozor/blog/3331/ (Дата обращения: 08.01.2024)

УДК 004.056

Степанов Максим Олегович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ

Нагаев Назим Харисович, научный руководитель, старший преподаватель кафедры «Системы информационной безопасности»
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, student
Kazan National Research Technical University named after A.N. Tupolev-KAI

Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer at the Department of Information Security Systems
Kazan National Research Technical University named after A.N.

Tupolev-KAI
Russia, Kazan

Исследование инфраструктуры открытых ключей

Public Key Infrastructure Research

Аннотация: В данной статье детально рассматривается критически важный компонент обеспечения информационной безопасности – Public Key Infrastructure (PKI). Особое внимание уделяется основным компонентам, а также ключевым задачам PKI. Несмотря на надежность и эффективность PKI, существуют потенциальные уязвимости, которые могут быть использованы злоумышленниками. В статье обсуждаются наиболее распространенные уязвимости PKI. Отмечается критическая важность для обеспечения безопасности в цифровом мире и отмечается, что PKI будет продолжать развиваться и совершенствоваться.
Ключевые слова: Инфраструктура открытых ключей (PKI), центр сертификации (CA), цифровой сертификат, информационная безопасность.
Abstract: This article examines in detail the critical component of information security – Public Key Infrastructure (PKI). Special attention is paid to the main components, as well as the key tasks of the PKI. Despite the reliability and effectiveness of the PKI, there are potential vulnerabilities that can be exploited by attackers. The article discusses the most common PKI vulnerabilities. The critical importance for ensuring security in the digital world is noted and it is noted that PKI will continue to develop and improve.
Key words: Public Key Infrastructure (PKI), Certification Authority (CA), digital certificate, information security.

Инфраструктура открытых ключей (PKI) - это набор ролей, политик, аппаратного обеспечения, программного обеспечения и процедур, необходимых для создания, управления, распространения, использования, хранения и отзыва цифровых сертификатов и управления шифрованием с открытым ключом. Целью PKI является облегчение безопасной электронной передачи информации для целого ряда сетевых операций, таких как электронная коммерция, интернет-банкинг и конфиденциальная электронная почта. Это требуется для действий, в которых простые пароли являются неадекватным методом аутентификации и требуются более строгие доказательства для подтверждения личности сторон, участвующих в общении, и для проверки достоверности передаваемой информации [1]. Эта технология играет ключевую роль в обеспечении безопасности электронных транзакций, аутентификации пользователей, защите конфиденциальной информации и многих других областях.

PKI состоит из следующих основных компонентов [2,3]:

Центр сертификации (CA)

Центр сертификации (Certificate Authority) является доверенным учреждением, ответственным за выдачу, подпись и управление цифровыми сертификатами. Основные функции CA включают в себя:

– Выдача сертификатов: CA проверяет подлинность заявок на сертификаты и подписывает их, предоставляя доказательство подлинности открытого ключа, связанного с конкретным субъектом.

– Отзыв сертификатов: В случае утери секретного ключа или компрометации сертификата, CA имеет возможность отозвать сертификат, предотвращая его дальнейшее использование.

– Обновление сертификатов: CA также отвечает за переоценку и обновление сертификатов при необходимости, например, при истечении срока действия сертификата.

Цифровые сертификаты

Цифровые сертификаты являются основным инструментом PKI и используются для аутентификации и обмена ключами между участниками системы. Они содержат следующие основные элементы:

– Открытый ключ: Сертификат содержит открытый ключ, который является публичным компонентом криптографического ключевого пары и используется для шифрования или проверки цифровых подписей.

– Идентификационная информация: В сертификате также содержится информация о владельце сертификата (субъекте), включая имя, адрес электронной почты и другие идентификационные данные.

– Подпись CA: Цифровой подписью CA подтверждается подлинность содержимого сертификата, обеспечивая доверие к его содержанию и открытому ключу, который он содержит.

Серверы и клиенты

Серверы и клиенты используют цифровые сертификаты для аутентификации друг друга и обмена зашифрованными данными. При установлении защищенного соединения, например, по протоколу SSL/TLS, клиенты проверяют подлинность сертификата сервера, а серверы - сертификаты клиентов.

Криптографические алгоритмы

PKI использует различные криптографические алгоритмы для различных целей, таких как генерация ключей, шифрование данных и создание цифровых подписей. Эти алгоритмы включают в себя RSA, DSA, ECDSA, AES, SHA и многие другие, каждый из которых имеет свои преимущества и области применения в PKI.

Инфраструктура открытых ключей выполняет целый ряд ключевых задач, которые являются фундаментальными для обеспечения безопасности электронных коммуникаций, аутентификации и защиты данных.

Одной из важнейших задач PKI является аутентификация. PKI предоставляет механизмы, которые позволяют участникам проверять подлинность друг друга. Цифровые сертификаты, выданные доверенными центрами сертификации (CA), используются для проверки подлинности участников системы.

Другая важная задача - шифрование данных. PKI использует криптографические методы для шифрования информации, обеспечивая конфиденциальность во время ее передачи через открытые сети, такие как интернет. Это гарантирует, что данные остаются защищенными от несанкционированного доступа.

Цифровые подписи также являются важной частью PKI. Они представляют собой цифровой аналог обычной ручной подписи и обеспечивают подлинность и целостность данных. Благодаря цифровым подписям стороны могут проверить, что данные не были изменены после их подписания.

Управление ключами - еще одна приоритетная задача PKI. Это включает в себя генерацию, хранение и управление криптографическими ключами, которые используются для шифрования данных и создания цифровых подписей. Также важно обеспечить ротацию, резервное копирование и управление доступом к ключам.

Создание и управление цифровыми сертификатами также входит в обязанности PKI. Цифровые сертификаты играют ключевую роль в аутентификации и шифровании данных. PKI включает в себя процессы создания, подписи и распространения цифровых сертификатов, содержащих открытые ключи и идентификационную информацию о владельце сертификата.

Наконец, PKI позволяет устанавливать политики безопасности и управлять доступом к защищенным ресурсам. Это включает определение прав доступа, аутентификацию пользователей и авторизацию операций.

В общем, задачи PKI связаны с обеспечением безопасности, конфиденциальности и целостности данных в сети, обеспечивая аутентификацию участников и защиту информации от несанкционированного доступа и модификации.

Хотя Public Key Infrastructure (PKI) представляет собой эффективный механизм обеспечения безопасности, имеются потенциальные слабые места, которые могут быть использованы злоумышленниками. Некоторые из основных уязвимостей в PKI включают:

Утрата или компрометация закрытых ключей цифровых сертификатов может привести к серьезным нарушениям информационной безопасности. Злоумышленники могут использовать скомпрометированные закрытые ключи для подделки сертификатов, атак типа "Man-in-the-Middle" или дешифровки зашифрованных данных.

Злоумышленники могут также создавать поддельные сертификаты, которые выдаются от имени доверенного центра сертификации (CA). Это может привести к тому, что пользователи будут доверять фальшивым сертификатам и передавать конфиденциальные данные злоумышленникам.

Часто применяются методы социальной инженерии, которые могут быть направлены на обман пользователей или администраторов PKI [4]. Эти атаки могут привести к компрометации секретных ключей или сертификатов. Например, злоумышленники могут пытаться убедить пользователей предоставить свои личные данные или секретные ключи, выдавая себя за доверенные лица или запрашивая информацию под предлогом доверенных запросов.

Если ключи и сертификаты не обновляются регулярно, это может создать возможность для атак на основе устаревших криптографических методов или скомпрометированных ключей.

Приложения или системы, не осуществляющие проверку цифровых сертификатов на предмет отзыва или подлинности, могут привести к снижению безопасности и нарушению конфиденциальности.

Недостаточная безопасность у доверенного центра сертификации (CA) может привести к угрозе компрометации всей инфраструктуры PKI и возможности создания поддельных сертификатов.

С ростом зависимости современных бизнес-моделей от электронных транзакций и цифровых документов, а также с увеличением числа устройств с поддержкой Интернета, подключаемых к корпоративным сетям, роль инфраструктуры открытых ключей (PKI) выходит за рамки отдельных систем. В настоящее время PKI должны поддерживать большее количество приложений, пользователей и устройств в сложных экосистемах. Кроме того, из-за более строгих государственных и отраслевых стандартов безопасности данных основные операционные системы и бизнес-приложения, как никогда ранее, полагаются на корпоративную PKI для обеспечения доверия.

Заключение. Public Key Infrastructure (PKI) является критически важным компонентом обеспечения безопасности в современных электронных коммуникациях и транзакциях. PKI обеспечивает аутентификацию, конфиденциальность и целостность данных, а также управление ключами и цифровыми сертификатами. Несмотря на потенциальные уязвимости, PKI остается надежной и эффективной системой для обеспечения безопасности в цифровом мире. По мере развития технологий и появления новых угроз безопасности, PKI будет продолжать адаптироваться и совершенствоваться, чтобы соответствовать меняющимся требованиям.

Библиографический список:

1. Инфраструктура открытых ключей - Abcdef . Wiki [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Public_key_infrastructure (Дата обращения: 25.02.2024)
2. Основные компоненты инфраструктуры с открытыми ключами: [Электронный ресурс]. URL: https://www.osp.ru/lan/2002/01/135678 (Дата обращения: 25.02.2024)
3. The Public Key Infrastructure Approach to Security: [Электронный ресурс]. URL: https://docs.oracle.com/cd/A97630_01/network.920/a96582/pki.htm (Дата обращения: 25.02.2024)
4. Степанов М.О. Социальная инженерия: методы атак и способы предотвращения // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XXVII Международной научнопрактической конференции, Москва, 25 января 2024 года. –Москва. Печатный цех, 2024 – С. 35-41. (Дата обращения: 25.02.2024)
5. Что такое PKI? Главное об инфраструктуре открытых ключей: [Электронный ресурс]. URL: https://habr.com/ru/articles/655135/ (Дата обращения: 25.02.2024)

УДК 004.056

Степанов Максим Олегович, студент
Лукьянов Эмиль Радикович, студент
Мисбахов Нияз Ильясович, студент
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ

Нагаев Назим Харисович, научный руководитель, старший преподаватель кафедры «Системы информационной безопасности»
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ
Россия, г. Казань

Stepanov Maxim Olegovich, student
Lukyanov Emil Radikovich, student
Misbakhov Niyaz Ilyasovich, student
Kazan National Research Technical University named after A.N. Tupolev-KAI

Nagaev Nazim Kharisovich, scientific supervisor, senior lecturer at the Department of Information Security Systems
Kazan National Research Technical University named after A.N. TupolevKAI
Russia, Kazan

Использование искусственного интеллекта и машинного обучения для обнаружения и защиты от атак

Using artificial intelligence and machine learning to detect and defend against attacks

Аннотация: Данная статья посвящена использованию искусственного интеллекта и машинного обучения для защиты информации от киберугроз. В ней рассматриваются современные подходы и методы, применяемые для обнаружения и защиты от атак. Подчеркиваются преимущества этих технологий и их вклад в обеспечение информационной безопасности. В статье анализируются существующие решения, использующие искусственный интеллект и машинное обучение, а также перспективы их развития и возможности для создания более надежных систем защиты.
Ключевые слова: искусственный интеллект, машинное обучение, обнаружение атак, защита от атак, информационная безопасность.
Abstract: This article is devoted to the use of artificial intelligence and machine learning to protect information from cyber threats. It examines modern approaches and methods used to detect and protect against attacks. The advantages of these technologies and their contribution to information security are emphasized. The article analyzes existing solutions using artificial intelligence and machine learning, as well as the prospects for their development and opportunities for creating more reliable protection systems.
Keywords: artificial intelligence, machine learning, attack detection, attack protection, information security.

С развитием информационных технологий и расширением цифровизации в различных сферах жизни, вопросы информационной безопасности становятся все более актуальными и приобретают особое значение в нашей жизни. Традиционные методы защиты, такие как антивирусы и межсетевые экраны, становятся недостаточно эффективными для борьбы с новыми и сложными атаками. Злоумышленники постоянно совершенствуют свои методы, и традиционные средства защиты не всегда могут их обнаружить и предотвратить. В свете этого развивается

повышенная актуальность применения искусственного интеллекта и машинного обучения для обеспечения обнаружения и защиты от атак

Искусственный интеллект и машинное обучение - это области компьютерных наук, которые изучают разработку систем, способных выполнять задачи, обычно требующие человеческого интеллекта. Машинное обучение позволяет компьютерам "учиться" на основе опыта, а искусственный интеллект позволяет им принимать решения и делать прогнозы на основе этих данных [1].

Использование искусственного интеллекта и машинного обучения в обнаружении аномалий в информационных системах представляет собой современный подход, который автоматизирует процесс выявления необычных событий и анализа безопасности. Эти технологии способны обрабатывать большие объемы данных, такие как сетевой трафик, журналы событий и системные логи, для выявления подозрительных паттернов поведения, которые могут остаться незамеченными человеческим глазом. Обнаружение аномалий может включать в себя неожиданные изменения в сетевом трафике, необычные запросы к базам данных или аномальные действия пользователей. Выявление таких аномалий может свидетельствовать о потенциальных кибератаках или вторжениях, что позволяет оперативно принимать меры по их предотвращению.

Искусственный интеллект и машинное обучение также играют ключевую роль в классификации и распознавании различных типов атак. С их помощью можно создавать модели, которые способны распознавать различные виды атак, такие как DDoS-атаки, вирусы, вредоносное ПО и другие. Это позволяет быстро и точно определить тип атаки, что в свою очередь позволяет быстро реагировать и применять соответствующие меры защиты.

Одним из наиболее перспективных применений искусственного интеллекта и машинного обучения в кибербезопасности является способность прогнозировать будущие угрозы. Алгоритмы машинного обучения могут анализировать исторические данные о кибератаках, выявлять паттерны и тенденции и использовать эти данные для прогнозирования вероятности и характера будущих атак. Это позволяет организациям принимать необходимые меры и усиливать свою защиту против предполагаемых угроз [2].

Искусственный интеллект и машинное обучение позволяют создавать адаптивные системы защиты, способные учиться на основе новых угроз и атак, адаптируя свои методы обнаружения и защиты для эффективного противостояния новым видам атак.

Искусственный интеллект может помочь определить приоритет угроз в реальном времени, учитывая их потенциальное воздействие на систему и важность защищаемых ресурсов, а затем система автоматически принимает

решения о мерах защиты, таких как блокировка подозрительного трафика или отключение уязвимых узлов. В случае успешного вторжения искусственный интеллект и машинное обучение могут автоматически запускать процессы отката системы к предыдущему рабочему состоянию, минимизируя ущерб от атаки.

Искусственный интеллект также способен улучшить системы биометрической аутентификации, обеспечивая более точное распознавание лиц, отпечатков пальцев и других биометрических данных. Машинное обучение может анализировать обычные паттерны поведения пользователей, позволяя системам быстро обнаруживать аномалии и потенциальные попытки несанкционированного доступа. Искусственный интеллект может помочь создать более сложные и интеллектуальные методы многофакторной аутентификации, учитывая контекст использования, такие как местоположение пользователя или время доступа.

Рассмотрим несколько примеров современных решений, которые используют искусственный интеллект и машинное обучение для обнаружения и защиты от атак [3]:

Системы обнаружения вторжений (Intrusion Detection Systems, IDS) применяют методы искусственного интеллекта и машинного обучения для анализа сетевого трафика и выявления аномального поведения, свидетельствующего о возможной вредоносной активности или атаке.

Анализаторы вредоносных программ используют искусственный интеллект и машинное обучение для анализа кода и поведения программ с целью обнаружения вредоносных программ, таких как вирусы, трояны и шпионское ПО.

Системы предотвращения утечки данных (Data Loss Prevention, DLP) также опираются на технологии искусственного интеллекта и машинного обучения для мониторинга и обнаружения попыток несанкционированного доступа или утечки конфиденциальной информации.

Системы анализа журналов и событий (Log and Event Analysis Systems) используют современные алгоритмы для анализа журналов и событий, регистрируемых в информационных системах, с целью обнаружения аномального поведения и потенциальных угроз.

Антивирусные программы успешно используют искусственный интеллект и машинное обучение для обнаружения и блокировки новых и неизвестных вирусов и вредоносных программ.

Системы угрозы интеллектуальной безопасности (Threat Intelligence Systems) используют данные из различных источников и технологии машинного обучения для анализа и предоставления информации о новых угрозах и методах атак.

Системы автоматического реагирования на угрозы используют искусственный интеллект для автоматического реагирования на

обнаруженные угрозы. Они могут принимать мгновенные меры по блокированию атакующих IP-адресов, ограничению доступа к ресурсам и другим действиям для минимизации ущерба от атаки.

Это лишь некоторые примеры современных решений, которые используют искусственный интеллект и машинное обучение для обнаружения и защиты от атак. Технологии в этой области продолжают развиваться, и новые инновационные решения появляются с каждым годом.

Перспективные направления развития в сфере искусственного интеллекта и машинного обучения для обнаружения и защиты от кибератак также привлекают внимание исследователей и специалистов.

В данной области можно выделить два направления развития технологий.

Одно из направлений - улучшение точности обнаружения. Исследования в этой сфере направлены на разработку новых алгоритмов обучения и использование более сложных моделей, чтобы повысить точность обнаружения атак и снизить количество ложных срабатываний. Также важным фактором является улучшение качества данных, используемых для обучения моделей.

Другое направление, которое заслуживает внимания, - это автоматическое обучение. Научные исследования в данной области стремятся разработать способы, позволяющие моделям автоматически обучаться без необходимости ручной настройки параметров и выбора признаков. Это значительно упрощает процесс развертывания систем обнаружения и защиты, делая его более эффективным и доступным для широкого круга пользователей. Автоматическое обучение основано на принципе автономного обучения моделей без участия человека. В основе этого подхода лежит использование алгоритмов, которые способны самостоятельно адаптироваться к изменяющимся условиям и оптимизировать свои параметры на основе обратной связи от среды.

Эти направления исследований будут способствовать развитию более эффективных и надежных систем обнаружения и защиты от атак, что является критически важным в условиях, когда количество угроз постоянно возрастает, и хакеры постоянно совершенствуют свои методы.

Заключение. Использование искусственного интеллекта и машинного обучения в области информационной безопасности стало важным шагом в борьбе с кибератаками. Эти технологии автоматизируют анализ больших объемов данных, выявляют аномалии и возможные угрозы в режиме реального времени, а также адаптируются к изменяющимся условиям. Интеграция искусственного интеллекта и машинного обучения способствует сокращению времени реагирования на угрозы, повышению точности обнаружения и снижению рисков для организаций и конечных пользователей. В дальнейшем исследования в этой сфере будут направлены

на разработку более сложных моделей и оптимизацию применения данных технологий в реальных условиях.

Библиографический список:

1. Искусственный интеллект и машинное обучение в кибербезопасности – прогноз на будущее: [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity (Дата обращения: 26.02.2024)
2. Машинное обучение и искусственный интеллект в сфере кибербезопасности.: [Электронный ресурс]. URL: https://airobotic.ru/mashinnoe-obuchenie-i-iskusstvennyj-intellekt/mashinnoe_obuchenie_i_iskusstvennyj_intellekt_v_sfere_kiberbezopasnosti/ (Дата обращения: 26.02.2024)
3. Искусственный интеллект в кибербезопасности: обнаружение и предотвращение кибератак: [Электронный ресурс]. URL: https://nauchniestati.ru/spravka/obnaruzhenie-i-predotvrashhenie-kiberatak-s-pomoshhyu-ii/ (Дата обращения: 26.02.2024)
4. How Security Analysts Can Use AI in Cybersecurity [Электронный ресурс]. URL: https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/ (Дата обращения: 26.02.2024)

Педагогические науки

УДК 372.8

Боряева А. И. студент бакалавриата
ФГБОУ ВО «Нижегородский государственный лингвистический университет им. Н. А. Добролюбова»
Россия, Нижний Новгород

Хомова Н. А., к.п.н. доцент кафедры поливального обучения и международного бакалавриата ИДО
ФГБОУ ВО «Нижегородский государственный лингвистический университет им. Н. А. Добролюбова»
Россия, Нижний Новгород

Boryaeva A.I. undergraduate student
Federal State Budgetary Educational Institution of Higher Education "Nizhny Novgorod State
Linguistic University named after. N. A. Dobrolyubova"

Russia, Nizhny Novgorod

Khomova N. A., Ph.D. Associate Professor of the Department of Irrigation training and international baccalaureate IDO
Federal State Budgetary Educational Institution of Higher Education "Nizhny Novgorod State Linguistic University named after. N. A. Dobrolyubova"
Russia, Nizhny Novgorod

Психологический аспект процесса формирования грамматического навыка у обучающихся на уровне среднего общего образования

Psychological aspect of the process of forming grammatical skills in students at the level of secondary general education

Аннотация: в данной статье рассматривается психологический аспект формирования грамматического навыка в иностранном (английском языке) на уровне среднего общего образования. Наиболее сложным аспектом обучения английскому языку, как с точки зрения психологии, так и педагогики, всегда являлась грамматика. Причина этого заключается в абсолютном несоответствии грамматических систем русского и английского языков. Особо остро эта проблема ощущается на уровне общего среднего образования, где обучающиеся пытаются найти связь грамматики английского языка с русским. Целью преподавателя является выбрать наиболее подходящую и легко распознаваемую и запоминающуюся единицу презентации любого грамматического явления. Для этого необходимо подробнее ознакомиться с психологическим аспектом формирования грамматического навыка.

Ключевые слова: психологический аспект, грамматический навык, коммуникативно-функциональный подход, рецептивный навык, продуктивный навык, упражнения, лингвокогнетивные особенности, синтаксические грамматический навыки, морфологический грамматические навыки, генеративная лингвистика, генеративная грамматика.

Annotation: this article examines the psychological aspect of the formation of grammatical skills in a foreign language (English) at the level of secondary general education. The most difficult aspect of teaching English, both from the point of view of psychology and pedagogy, has always been grammar. The reason for this is the absolute discrepancy between the grammatical systems of the Russian and English languages. This problem is particularly acute at the level of general secondary education, where students are trying to find a connection between English grammar and Russian. The teacher's goal is to choose the most appropriate and easily recognizable and memorable presentation unit for any grammatical

phenomenon. To do this, you need to learn more about the psychological aspect of the formation of grammatical skills.

Key words: psychological aspect, grammatical skill, communicative and functional approach, receptive skill, productive skill, exercises, linguistic cognitive features, syntactic grammatical skills, morphological grammatical skills, generative linguistics, generative grammar.

Структура грамматической компетенции включает продуктивные и рецептивные грамматические навыки. «Рецептивные грамматические навыки – это навыки узнавания и понимания грамматических явлений в разных типах текстов (устных и письменных) при владении материалом, как активном, так и пассивном. При активном владении материалом рецепция опирается на речевые автоматизированные связи слухоречемоторных образов и значений и зрительно-графемных речемоторнослуховых образов и значений, то есть при аудировании и чтении. При пассивном владении материалом рецептивный навык базируется на чтении иностранных текстов, языковым материалом которого читатель не владеет активно и может лишь узнавать его на основе зрительной памяти, в основе этого вида навыков лежат автоматизированные процессы узнавания языковых явлений и понимания их значения.» [6]

Без сформированных грамматических навыков немыслимо формирование умений всех типов речи: аудирование, письмо, говорение, чтение.

На уровне школьного образования базовый минимум грамматических средств изучается концентрически. На этапах старшего и профессионально ориентированного образования ряд конструкций и явлений может усваиваться, как продуктивный, на младшем и среднем – как рецептивный.

С помощью коммуникативно-функциональных признаков проводится систематизация грамматических средств. На отбор грамматического минимума влияют источники и принципы отбора.

Если говорить об источниках отбора, то из диалогических образцов текстов, которые были написаны носителями языка, а также из образцов звучащей речи, производится отбор продуктивной грамматики.

Принципы отбора могут быть следующими:

- по образцовости,
- по коэффициенту стабильности,
- по исключению синонимов.

В свою очередь, рецептивный грамматический минимум отбирается из таких печатных источников, где содержатся примеры книжно-письменной речи. Перечислим основные принципы, лежащие в основе отбора:

- многозадачность,

- распространённость и частотность в источниках (печатных и книжных), то есть коэффициент стабильности.

Овладение данными средствами требует значительного количества практики реального речевого общения. Таким образом, научение происходит в рамках отражения учебной ситуации, имитирующей процесс реального общения и в рамках коммуникативной деятельности, требующей применения грамматических средств.

Перечислим основные аспекты обучения грамматике, исходя из коммуникативно-функционального подхода.

Во-первых, учебный материал должен включать в себя демонстрацию использования языка в естественной среде.

Во-вторых, предоставляемый материал должен быть чётко структурирован и в нём должны выделяться семантические, формальные и функциональные аспекты.

В-третьих, грамматический материал должен быть представлен в полном объёме для того, чтобы произошло закрепление полученных навыков и информации в разных контекстах.

В-четвёртых, необходима иллюстративная наглядность предлагаемого материала в виде схем, таблиц, рисунков и т.д., а также следует систематически повторять пройденный материал для его лучшего закрепления.

В-пятых, все пояснения и правила должны понятно и точно отражать специфику предоставляемого материала.

В-шестых, для лучшего закрепления изучаемых грамматических явлений необходимо чередовать различные виды работ и общения (групповая работа, индивидуальная, парная и т.д.).

Ознакомление с новым материалом происходит в несколько этапов:

1. Первым этапом является ознакомление.
2. После него следует этап первичного закрепления.
3. Третьим этапом является развитие умений и навыков использования грамматики в процессе коммуникации при письменном и устном общении.

«При составлении индивидуального учебного плана, очевидно, необходимо учитывать сложность материала, интерес учеников к предмету и их уровень подготовленности в данной области. Следует также проводить большую предварительную работу, а именно» [5]:

- необходимо работать с учащимися и развивать у них такой навык, как планирование собственной деятельности;
- нужно работать над выработкой у учащихся навыков рационализации времени и усилий, требуемых для выполнения работ, задаваемых на дом;
- требуется проводить подробный инструктаж учащихся о том, как именно следует выполнять задания и порядке их распределения;

- следует осуществлять контроль деятельности учащихся, выявлять допущенные ошибки и работать над ними;

- наконец, важным является поощрение учеников к процессу обучения и представление разумных стимулов.

Благодаря данным действиям можно добиться улучшения качества учебного процесса, а также повышения показателей эффективности учебной деятельности, происходящей за счет более ускоренного обучения и прохождения учебной программы, увеличения времени для экспериментальных, исследовательских и практических работ и активизации творческого развития.

В качестве важного этапа обучения и изучения грамматики выступают упражнения. Этап упражнений задействует различные языковые средства и подразумевает практику их применения и накопления в процессе коммуникации.

Перечислим требования, предъявляемые к упражнениям:

1. Одноцелевое применение упражнения. Подразумевается, что упражнение, во-первых, должно быть представлено на знакомой обучающемуся лексике, а во-вторых, в нём содержится только одно явление грамматики.

2. Упражнение должно включать в себя простые и наглядные образцы, благодаря которым обучающийся сможет понять, что именно от него требуется в рамках данного задания.

3. Лучше всего позволяют усвоить знания и закрепить навыки упражнения, в которые включены проблемные и коммуникативные задачи. Таким образом, следует избегать простых механических приёмов и заучивания.

Перечислим основные типы подготовительных упражнений. К ним относятся упражнения:

- в субституции;
- на дифференциацию и узнавание явлений грамматики;
- в трансформации;
- переводные;
- репродуктивные;
- вопросно-ответные.

Рассмотрим каждый из этих типов более подробно.

1. Упражнение в субституции. Здесь предполагается образование предложений, при этом следует обращать внимание на форму применяемых причастий. Можно предложить составить идентичную таблицу, но задействовать в ней другие примеры.

2. Упражнение в дифференциации и узнавании.

Приведем примеры таких упражнений:

- попробуйте на слух определить предложение, в котором содержится новое явление грамматики. Воспроизведите данное предложение;

- руководствуясь формальными признаками структуры грамматики и обобщающим правилом, заполните таблицу;

- прочитайте предложенный текст и выделите в нем грамматический материал, отображающий правила, указанные в инструкции к данному заданию;

- прочитайте текст и проанализируйте те грамматические явления, которые в нем содержатся;

- к указанным структурам подберите грамматические замены;

- сопоставьте элементы предложений, находящиеся в разных столбцах.

3. Упражнения в трансформации. К таким упражнениям могут быть отнесены следующие:

- осуществите преобразование залогов и поясните осуществляемые действия;

- осуществите преобразование простых предложений при помощи предложенных союзов, составив одно сложное предложение из двух простых;

- осуществите преобразование диалогической формы речи в монологическую. При этом необходимо сохранить предлагаемые количественные данные;

- осуществите преобразование предложений повествовательного типа в вопросительные предложения.

4. Переводные упражнения. К таким упражнениям можно отнести, например, следующие:

- осуществите перевод мини-текста или предложения на русский язык с другого языка (в указанных текстах и предложениях содержатся языковые явления или грамматические явления, над которыми ведется работа);

- осуществите обратный перевод.

5. Репродуктивные упражнения. К такому типу упражнений можно отнести следующие:

- в предлагаемом диалоге содержатся изучаемые грамматические явления. Осуществите сокращение, дополнение или иное изменение предложенного диалога;

- прочитайте предложенный текст. Задайте вопросы к данному тексту и перескажите его, основываясь на составленных вопросах;

- осуществите пересказ предложенного текста, предварительно заполнив глаголами пропущенные места.

6. Вопросно-ответные упражнения. К таким упражнениям можно отнести:

- разбейтесь на пары и узнайте у своего собеседника какой-либо аспект, например, о том, как он провел вчерашний день:

- руководствуясь предложенной схемой и образцами, задайте вопросы своему собеседнику;

- игровая деятельность, которая предполагает необходимость составления вопросов, исходя из предложенного рисунка, схемы, текста и т.д.

При формировании глубинных и поверхностных синтаксических структур языка у обучающихся были выявлены некоторые сложности. А именно, при формировании поверхностных синтаксических структур языка, которые непосредственно участвует в грамматическом оформлении готовой речевой продукции, выявлены следующие проблемы: неправильное использование глагольного времени, неправильное использование инфинитива, нарушения падежной парадигмы в составе синтаксической конструкции, неверное использование категории рода, неверное использование грамматического числа, смешение границ предложений (входящих в исследуемый текст).Что касается формирования глубинных синтаксических структур языка, которые позволят отразить смысловую близость ряда предложений, содержащих одни и те же лексические единицы и отличающиеся некоторыми грамматическими значениями, то были выявлены следующие трудности: неверное использование союзов, как подчинительных, так и сочинительных, несоблюдение грамматических норм языка, искажение смысла синтаксической конструкции, не использование сложных синтаксических моделей (замена их на пару более простых), неверное вычленение глубинного смысла, опора на денотативные признаки понятий в процессе анализа предложений, принятие неверных решений, основанных на апелляции к собственному опыту, нарушение процесса декодирования квази предложений, содержащих грубое искажение семантики [1].

Н. Хомский в своих трудах неоднократно говорил о теории генеративной лингвистики. Глубинные структуры – это ядерные синтаксические конструкции на уровне универсальной грамматики. Глубинными структурами являются элементы, которые изначально заложенные в сознании человека и представляют собой языковую компетенцию. Описание языка формальными моделями определенного типа являются опорой генеративной лингвистики. Основной тип таких моделей – трансформационные порождающие (генеративные) грамматики. Грамматику данного типа используют носители языка, чтобы понять и сформировать любое высказывание. Языковая компетенция и употребления языка – это два противопоставленных друг другу базовых понятия генеративной грамматики.

Генеративная грамматика подразделяется на три компонента (синтаксический, семантический и фонологический) и два уровня (глубинный и поверхностный). Наша речь и поверхностные структуры, порождаемые с помощью преобразований, находятся на поверхностном

уровне, на глубинном уровне, соответственно, располагаются глубинные структуры. Поверхностные синтаксические структуры создает трансформационный компонент из структур, полученных с помощью работы базовых правил. Выявлено около двух десятков моделей трансформаций, необходимых для создания множества инвариантов, употребляемых в речи, среди которых: отрицание, пассивизация, трансформация вопроса. Следующий компонент – фонологический, то есть фонетическая интерпретация предложения.

Теория генеративной лингвистики неоднократно подвергалась различным изменениям, как самим автором (Н. Хомским), так и другими исследователями, но, несмотря на это в ней сохранились некоторые фундаментальные положения. Первое, врожденный характер способности понимать и воспроизводить грамматику родного языка, то есть с помощью ограниченного набора грамматических структур человек может создавать неограниченное количество предложений. Второй, универсальная грамматика, то есть человек, овладевший языком, усваивает его правила и систему [1].

Отличительной особенностью языковой системы и составляющих ее компонентов является наличие в ней, помимо грамматического порядка «интенциональности» или «языкового смысла». Это становится наиболее понятным при рассмотрении правильно построенных, но неверных по смыслу утверждений, таких как, «Светлячок поймал девочку», «Colorless green ideas sleep furiously» или «Нам навстречу летели озера». Под ложностью в данном случае мы подразумеваем не отсутствие смысла вообще, но его намеренное искажение (mutilation) или неадекватность (inadequacy). Схема построения такого рода поверхностных структур будет отличаться от классической схемы построения, предложенной Д. Слобиным и Дж. Грином.

Эти отличия, главным образом, состоят в изменении направленности взаимоотношений поверхностной и глубинной. Так, например, в первом предложении «Светлячок поймал девочку», результирующая поверхностная структура оказывает обратное воздействие на глубинную структуру, как с точки зрения реципиента, так и самого отправителя информации [6].

Представим обе структуры в виде соотношения базовых компонентов Sds + Vds + Ods и Sss + Vss + Oss, где Sds, Vds и Ods – субъект, действие и объект глубинной структуры, а Sss + Vss + Oss – субъект, действие и объект поверхностной структуры соответственно.

Перекрестность во взаимоотношениях является следствием реверсивного влияния поверхностной структуры на глубинную и соответствующей лексико-грамматической трансформации (SdsOss, OdsSss). Во втором предложении «Colorless green ideas sleep furiously» обратное влияние глубинной структуры на поверхностную также имеет место, однако,

за отсутствием третьего базового компонента Ods и, соответственно, Oss, отношения структур являются последовательно параллельным, а не перекрестными. Наличие определения и обстоятельство образа действия в данном случае можно считать нерелевантным, из-за их незначительного влияния на результирующий смысл.

Изучение грамматики невозможно представить без лексики. Несмотря на то, что в рамках генеративной лингвистики лексические единицы, уходят на второй план, при обучении школьников, использование известных лексических единиц крайне важно. На уровне основанного общего образования обучающемуся значительно легче воспринимать и оперировать новыми грамматическими конструкциями на базе уже изученной им ранее лексики.

Ментальный лексикон представляет собой сложное когнитивное образование, которое формируется в процессе усвоения человеком родного языка и представляет собой «динамическую функциональную систему, самоорганизующуюся вследствие постоянного взаимодействия между процессом переработки и упорядочивания речевого опыта и его продуктами» [3].

«Узлы и межузловые связи – структурные элементы современной модели ментального лексикона, представляющего его в виде многомерной ассоциативно-вербальной сети. Считается, что в ментальном лексиконе информация о каждом слове представлена дистрибутивным образом, то есть слово существует в виде набора взаимосвязей между несколькими или многими единицами сети, к изменению всего комплекса соотносимой с данным словом информации может привести изменение хотя бы одной из таких связей. Таким образом, язык в его «предречевой готовности» — это вся активированная информация, доступная для восприятия и продуцирования речи». [2]

Современные модели двуязычной грамматики основаны на предположении о том, что два языка представлены в ментальном пространстве индивида в виде единой интегрирующей сети, а освоение иностранного языка (Я2) происходит при активном участии родного языка (Я1).

Влияние этих двух языков осуществляется в двух направлениях: от Я1 к Я2 и, наоборот, от Я2 к Я1. При этом влияние иностранного языка на родной язык наблюдается не только в детском возрасте, когда система родного языка еще полностью не сформирована и не является стабильной, но и в ситуации обучения взрослых.

Из вышесказанного следует, что весь процесс освоения Я2 в большинстве случаев подразумевает бессознательное (или сознательное) установление сходства между единицами родного и иностранного языков. В результате в двуязычном ментальном лексиконе конструируется качественно

новая, универсальная категория, единицы которой обладают общим значением, одновременно принадлежат двум языкам и обеспечивают процессы межъязыкового взаимодействия [2].

Библиографический список:

1. Григорьева И.В., Аспекты теории глубинных структур в работах Н. Хомского, Вестник ВГУ, серия: Лингвистика и межкультурная коммуникация. 2018. № 4. С 9-12.
2. Доценко Т. И., Лещенко Ю. Е. Универсальные структуры и их функции в ментальном лексиконе билингва. 2013. 372с.
3. Ерофеева Е.В., Пепеляева Е.А. Структура семантического поля «человек» всознании носителей русского языка// Вестник Пермского Университета.Российская и зарубежная филология. Пермь, 2011. Вып.1(13). С.7-19.
4. Колякина Н.Г. Исследование уровня форсированности глубинных и поверхностных синтаксических структур языка у детей младшего школьного возраста с ОВЗ. 2018.
5. Хомова, Н.А., Галушкина А.А. Роль самостоятельной работы при обучении иностранному языку учащихся общеобразовательной школы на среднем этапе (6 класс) / Н. А. Хомова, А. А. Галушкина // Современные исследования: теория, практика, результаты: Сборник материалов Международной научно-практической конференции, Москва, 29 декабря 2023 года. – Москва: Центр развития образования и науки, ООО "Издательство АЛЕФ", 2023. – С. 12–20. – EDN SRWFTJ.
6. Формирование грамматических навыков у иностранных студентов-стоматологов. [Электронный ресурс]/ URL: https://cyberleninka.ru/article/n/formirovanie-grammaticheskih-navykov-u-inostrannyh-studentov-stomatologov. (дата обращения 22.02.2024).

DOI 10.34755/IROK.2024.29.33.022

УДК 378.1

*Габдуллина А. Ш.,*ст преподаватель
Санкт-Петербургский политехнический университет
Петра Великого (СПбПУ)
Россия, Санкт-Петербург

Gabdullina A. Sh., senior teacher
St. Petersburg Polytechnic University
Peter the Great (SPbPU)

Russia, Saint-Petersburg

Gabdullina A. Sh., senior teacher
St. Petersburg Polytechnic University
Peter the Great (SPbPU)
Russia, Saint-Petersburg
Gabdullina A. Sh., senior teacher
St. Petersburg Polytechnic University
Peter the Great (SPbPU)
Russia, Saint-Petersburg

Структурная геймификация: оптимальный баланс между игровыми элементами и академическими целями в обучении иностранным языкам

Structural gamification: optimal balance between game elements and academic goals in teaching foreign languages

Аннотация: Данная статья рассматривает концепцию структурной геймификации в контексте обучения иностранным языкам. Автор предлагает подход, основанный на достижении оптимального баланса между игровыми элементами и академическими целями. Структурная геймификация позволяет эффективно интегрировать игровые механики в образовательные процессы, стимулируя мотивацию и повышая уровень усвоения языковых навыков.
Ключевые слова: структурная геймификация, изучение иностранных языков, игровые элементы, академические цели, мотивация, языковые навыки.
Abstract: This article examines the concept of structural gamification in the context of teaching foreign languages. The author proposes an approach based on achieving an optimal balance between game elements and academic goals. Structural gamification allows you to effectively integrate game mechanics into educational processes, stimulating motivation and increasing the level of acquisition of language skills.
Keywords: structural gamification, foreign language learning, game elements, academic goals, motivation, language skills.

Современные университеты сталкиваются с серьезными вызовами в области мотивации и вовлеченности студентов в образовательный процесс. Геймификация, интегрируя игровые элементы в академическую среду, предоставляет возможность эффективного решения этих проблем. Однако,

для максимальной эффективности в высших школах важно более глубоко разобраться в сути геймификации и ее функциональности. В данной статье мы рассмотрим следующие вопросы: что такое геймификация, чем структурная геймификация отличается от содержательной, типы геймификации (частичная и полная), какие академические цели в геймификации и какой оптимальный баланс между игровыми элементами и академическими целями.

Согласно О.В. Орловой и В.Н. Титовой, геймификация может быть определена как стратегия, внедряющая инструменты игрового дизайна в неигровые контексты для управления поведением студента с целью привлечения и увлечения их активности в решении прикладных задач [1]. Это также представляет собой метод решения реальных проблем с использованием игровых элементов и стратегий. Е.В. Климкович отмечает, что геймификация представляет собой стратегию активизации интереса, внедрения игровых элементов в учебную среду [2]. Ее цель - создать уровень вовлеченности, аналогичный тому, который обычно характерен для игр и ролевых сценариев. Это адаптация игровых форм к реальным процессам. В рамках геймификации реальность сохраняет свою основную природу. Ключевым аспектом геймификации является то, что обучающиеся сохраняет свою индивидуальность, двигаться в направлении своей мотивации и внутренней цели, например, освоить иностранный язык. Внедрение элементов геймификации, таких как уровни, награды и рейтинги, усиливает вовлеченность студентов, активизируя их эмоциональный опыт.

Как утверждают ряд авторов (Г.Э. Емалетдинова, В.С. Цилицкий, Н.В.Шершукова) геймификация, ориентирована на перенос логики игры в образовательную сферу и эффективно применяется в высшем образовании для улучшения мотивации и вовлеченности студентов [3].

Геймификация применяется для улучшения обучения, позволяя студентам обогащать свои знания через метод проб и ошибок. Она предоставляет студентам увлекательные возможности для обучения, расширяя их знания и понимание предмета. Главные задачи внедрения геймификации включают улучшения конкретных навыков (креативности, коммуникабельности, критического мышления и мотивации), формулирование у студентов задач с ясной целью, поддержку активного участия, оптимизацию процесса обучения, воздействие на изменение поведения и социализацию. Как утверждают А.Ш. Габдуллина и А.В. Рубцова, использование игр в образовании может способствовать креативности, решению проблем и обучению в увлекательной форме. Они также мотивируют студентов, повышают интерес к предметам, снижают стресс у студентов, снимают языковой барьер, улучшают оценки и развивают когнитивные навыки [4].

К. М. Капп дает наиболее подробное определение геймификации с точки зрения использования принципов игровой механики и мышления, с целью увлечения студентов, стимулирования их мотивации, активизации процесса обучения и решения проблем. Он выделяет две формы геймификации: *содержательную*, которая предполагает изменения традиционных методов обучения с организацией процесса обучения в соответствии с выбранным игровым сценарием и его правилами, и *структурную*, включающую использование отдельных игровых элементов в учебном процессе [5]. В структурной геймификации выделяют три ключевых компонента: игровые элементы, такие как участники, уровни, задания и ресурсы; механика игры, которая определяет принципы взаимодействия этих элементов; и динамика игры, способствующая вовлеченности игроков. Геймификационные элементы могут проявляться в разнообразных формах и с разными компонентами, что позволяет их использование на различных этапах обучения иностранному языку [6].

Вслед за Каппом, выделивший две формы геймификации, Е.В. Карманова также отмечает два типа геймификации, называя их *тяжелой* и *легкой*. Под «тяжелой» понимается все основные аспекты геймификации, начиная от постановки целей и задач, заканчивая итоговым контрольным заданием. Данная форма требует сценарного погружения, создания увлекательной сюжетной линии, правил, ролей и уровней. *Легкая* геймификация, согласно Кармановой, осуществляется в рамках отдельных занятий, включая игровые механики и элементы, такие как конкурсы, проекты, командные практики и ролевые игры. Эта форма геймификации может регулярно применяться в обучении, но охватывает лишь часть целей [7].

По мнению М.А. Хлыбовой, эксперименты с использованием геймификации при обучении иностранному языку показывает, что командная деятельность, включающая в себя взаимоотношения участников игрового процесса, эффективно реализуют этот подход. Основной идеей здесь является предположение о том, что студентам интересно работать в команде, и это обеспечивает эффективные средства общения на иностранном языке [8]. Пример может служить командная работа студентов при создании глоссария, терминологического словаря или написания эссе. В данном случае использование структурной формы геймификации способствует повышение учебной мотивации студентов за счет новаторского подхода, соревновательного элемента и творческой активности. Преимущества внедрения структурной геймификации в области обучения включают постоянное оценивание включают постоянное оценивание прогресса, доступное в режиме онлайн. Каждый раз, завершая определенный этап материала, студент проходит тест, оценивающий его знания и переходит к

новому этапу. Такой подход способствует выявлению как сильных, так и слабых сторон каждого студента.

Как утверждают В.И. Погорелов, Д.В. Зимина и О.О. Козак, структурная геймификация наилучшим образом соответствует обучению технических дисциплинам, в связи с небольшим объемом теории и большим количествам конкретных практических задач [9]. Однако, по нашему мнению, структурная геймификация также эффективно может быть применена и в обучении иностранным языкам, предоставляя возможность обучающимся перемещаться по учебному материалу с использованием игровых элементов без изменения его сути. В контексте изучения иностранных языков, структурная геймификация может стимулировать более активное участие студентов, создавать интересные сценарии для практики языковых навыков и обогащать обучение взаимодействием через игровые задачи. Таким образом, структурная геймификация представляет перспективный инструмент в обучении иностранным языкам, способствуя эффективному усвоению материала и поддерживая высокий уровень мотивации студентов.

В настоящее время многие преподаватели предпочитают применять структурную геймификацию, включающую элементы соревновательности, что способствует активному участию учащихся, а также создающую мотивацию через желание превзойти других и достичь высоких результатов [10]. Это также способствует развитию коммуникативных навыков, поскольку соревнование может включать в себя взаимодействие на иностранном языке, улучшая практическое применение изучаемого материала.

Геймификация может принимать разнообразные формы и выбор определяется преподавателем. Геймификация может применяться *как традиционный игровой подход* (ролевые игры, дискуссии, карточки, кроссворды и головоломки), так и в *цифровой среде* (компьютерные игры, обучающие мобильные приложения/ платформы, программы и приложения с элементами дополненной реальности) в обучении иностранным языкам.

Традиционный игровой подход обучение способствует формированию творческой и поисковой деятельности. Такой подход позволяет создавать мотивацию и интерес к изучению языка. Процесс обучения организован так, что преподаватель не прибегает к использованию каких-либо информационно-коммуникативных технологий.

Традиционный игровой подход может переходить к нетрадиционным формам и подходам, например, использование игровых механики с использованием цифровизации.

Сегодня существует достаточно большой выбор различных обучающих онлайн платформ (Moodle, SunRav BookOffice, LMS, Quizlet итд), компьютерных ресурсов и электронных платформ для создания обучающих игр. Создание таких программ или приложений требует от преподавателя,

помимо профессиональных качеств, определенной ИКТ-компетентности, а в некоторых случаях и базовых навыков программирования. Для создания качественных электронных продуктов, например обучающих видеоигр, могут использоваться различные языки программирования, такие как Lynx, Python, C++ и другие, или различные цифровые сервисы [11]. Однако, преимущество геймификации в том, что готовую базу можно использовать сколько угодно раз. Поэтому даже преподаватели иностранного языка могут с успехом использовать на своих занятиях ранее созданные обучающие игры, наполняя их новым контентом исходя из собственных потребностей. Множество программных сервисов и платформ с дидактическим потенциалом для геймификации обучения представляет собой обширный и разнообразный спектр.

Применения геймификации в обучении иностранному языку активизирует интерес обучаемых и стимулирует их вовлечение в учебную деятельность. Однако, за данным подходом стоят четкие академические цели, нацеленные на развитие языковых навыков. Академические цели обучения иностранного языка в геймификации включают в себя задачи, соответствующие образовательным стандартам и способствующие комплексному языковому развитию студентов. Одной из ключевых задач является: развитие лексического запаса, совершенствования навыков общения, стимулирование письменной и устной выразительности, развитие культурного понимания, стимулирование самостоятельного обучения [12]. Геймификация с успехом сочетает в себе игровые элементы и академические цели. Однако, необходимо применять оптимальный баланс между этими двумя аспектами, выделяя ключевые аспекты для сохранения академической серьёзности и предоставляя примеры успешной структурной геймификации в обучении иностранному языку. Такими ключевыми аспектами являются:

Целеполагание – геймификация должна быть выстроена вокруг образовательных целей, чтобы каждая игровая задача имела четкую академическую направленность;

Интеграция контента – игровые элементы должны взаимодействовать с учебным материалом, подчеркивая и укрепляя ключевые языковые концепции и навыки;

Оценивание – разработка эффективной системы оценки, которая отражает не только уровень учебных достижений, но и вовлеченность в геймифицированный процесс обучения;

Самостоятельное обучение – самостоятельное исследование языковых вопросов и решение задач самими студентами;

Структурность и прозрачность – структура геймификации должна быть понятной и прозрачной для студентов, чтобы они могли четко видеть, какие академические цели они достигают [13].

Как мы говорили ранее, одной из ключевых задач геймификации в обучении иностранным языкам является обогащение лексики. Включение новой лексики в сценарии игр способствует более глубокому усвоению материала, поскольку учащиеся не только учатся, но и применяют свои знания в контексте. Ролевые игры и групповые занятия позволяют учащимся не только изучать язык, но и использовать его в реальных ситуациях общения. Это развивает навыки языковой коммуникации и уверенность в использовании иностранного языка. Геймификация также направлена на углубление понимания языковых структур. Грамматические упражнения в игровой форме делают процесс обучения более приятными способствуют лучшему усвоению сложных грамматических конструкций. Кроме того, внедрение геймификации включает в себя стимулирование письменной и устной речи. Задача создания историй и диалогов на иностранном языке развивает творческие, грамотные и выразительные навыки [14].

Таким образом, несмотря на свой развлекательный характер, геймификация эффективно служит академическим целям обучения иностранному языку. Оптимальный баланс между игровыми элементами и академическими целыми в обучении языкам – это грамотное внедрение геймификации в учебный процесс.

Применения структурной геймификации в обучении иностранному языку приносит множество преимущества, начиная от эмоциональной вовлеченности и развития самостоятельности учащихся, до индивидуализации процесс обучения. Основным преимуществом являются беспредельные возможности в управлении мотивацией студентов, сокращении психологических трудностей, и улучшение усвоения материла.

Помимо преимуществ, геймификация обладает рядом недостатков. Она может вызывать краткосрочный эффект, так как студенты, быстро устают от игровых механик и других компонентов геймификации. Еще одним негативным аспектом в образовательной среде является возможность замещения учебного материала внешней формной геймификации, что может отвлечь внимание студентов от учебного материала. Для избежания этого, можно использовать структурную геймификацию, сочетать геймифицированные учебные занятия с традиционными. Наконец, резкое увеличение соревновательных элементов среди студентов может вызвать нестабильность и конфликты на занятии.

Для успешного применения структурной геймификации в обучение иностранных языков, необходимо решить технические и педагогические вопросы. Это включает в себя создание инновационных приложений и платформ.

В заключение, исследование структурной геймификации в обучении иностранным языкам выявило ее значительное влияние на современные образовательные практики. Элементы игры не только стимулируют мотивацию студентов и активно способствует усвоению языковых структур, но и снимает языковые барьеры, создает динамичное образовательное пространство, способствующее спешному освоению языка, адаптации к его структуре и развитию коммуникативных навыков.

Таким образом, структурная геймификация прочно вписывается в современный лингвистический контекст, обогащая образовательный процесс и поднимая его на новый уровень интерактивности и эффективности.

Библиографический список:

1. Орлова О. В., Титова В. Н. Геймификация как способ организации обучения // Вестник Томского государственного педагогического университета. 2015. No 9 (162). С. 60–64.
2. Климкович Е.В. Развитие геймификации образования в процессе реализации программ высшего и дополнительного образования // Современное педагогическое образование. 2021. №8. С.23-26.
3. Емалетдинова Г.Э., Цилицкий В.С., Шершукова Н.В. Геймификация как метод обучения :особенности и возможности// Московский экономический журнал. - 2022 (3). С. 702-708.
4. Габдуллина А.Ш., Рубцова А.В. Геймификация как средство развития гибких навыков и креативного мышления при обучении иностранному языку // Научно-методический электронный журнал «Концепт». – 2024. – № 2. С. 34–46.
5. Kapp K. M. The gamification of learning and instruction: game-based methods and strategies for training and education. New York: Pfieffer: An Imprint of John Wiley & Sons. Ideas into Practice. San Francisco: Wiley. - 2013. 480 p.
6. Гольцова Т. А., Проценко Е. А. Использование средств геймификации в процессе обучения иностранным языкам // Ярославский педагогический вестник. 2021. No 1 (118). С. 81-89.
7. Карманова Е.В. Тяжелая и легкая геймификация при обучении: что выбрать? / Е.В. Карманова, В.А. Шелеметьева // Информатика и образование. — 2020. — No 1(1). — С. 20–27.
8. Хлыбова М. А. Применение геймификации в процессе изучения иностранного языка в вузе / М. А. Хлыбова // Мир науки. Педагогика и психология. — 2022. — Т. 10. — No 1. С.3.
9. Погорелов В.И., Зимина Д.В., Козак О.О. Сравнительный анализ методов структурной и содержательной геймификации для создания электронного учебного курса. – Старт-2015: материалы Общероссийской

молодежной науч.- техн. конф. / Балт. гос. техн. ун-т. – СПб., 2015. – 64 с. (Библиотека журнала «Военмех. Вестник БГТУ», No25).
10. Быкадорова Е. С. Геймификация в образовании // Современные научные исследования и разработки. 2018. No 12 (29). С. 178–180.
11. Kapsargina S. A. Using the elements of gamification on LMS Moodle in the discipline of foreign language in a non-linguistic university / S. A. Kapsargina, Ju. A. Olentsova // Балтийский гуманитарный журнал. 2019. Т. 8. No 1 (26). С. 237-240.
12. Примерная программа дисциплины обучения иностранным языкам (в вузах неязыковых специальностей) // Федеральный портал «Российское образование». URL: http://www. edu.ru/db/portal/spe/progs/hf.01.01.htm (дата обращения: 05.01.2024).
13. Кармова М. Р. «Геймифицируй», или почему современному образованию нужны игры (на примере студентов, обучающихся по направлениям «Социология» и «Политология») // Гуманитарные науки. Вестник финансового университета. 2020. Т. 10. No 1. С. 46-50.
14. Богомолов А. И. Геймификация образовательно- процесса в высшем учебном заведении / А. И. Богомолов, В. П. Невежин // Новые информационные технологии в образовании : сб. науч. тр. / под ред. Д. В. Чистова. Москва : ООО «IC-Паблишинг», 2019. С. 129-131.

УДК 796.8

Пугачев Игорь Юрьевич
кандидат педагогических наук, доцент, доцент кафедры игровых и циклических видов спорта
ФГБОУ ВО «Тамбовский государственный университет имени Г.Р. Державина»
Россия, г. Тамбов

Парамзин Вячеслав Борисович, кандидат педагогических наук, доцент,
доцент кафедры физической подготовки
Краснодарское высшее военное училище имени
генерала армии С.М. Штеменко
Россия, г. Краснодар

Агабеков Назир Казанбекович, преподаватель
кафедры физической подготовки
Краснодарское высшее военное авиационное училище летчиков
имени А.К. Серова
Россия, г. Краснодар

Мацибурский Александр Викторович, доцент, старший преподаватель
кафедры физической подготовки
Краснодарское высшее военное авиационное училище летчиков
имени А.К. Серова
Россия, г. Краснодар

Pugachev Igor Yurievich, candidate of pedagogical sciences, associate professor, associate professor of the department of game and cyclic sports
Federal State Budgetary Educational Institution of Higher Education "Tambov State
University named after G.R. Derzhavin"
Russia, Tambov

Paramzin Vyacheslav Borisovich, candidate of pedagogical sciences, associate professor, associate professor of the department of physical training
Krasnodar Higher Military School named after
Army General S.M. Shtemenko
Russia, Krasnodar

Agabekov Nazir Kazanbekovich, teacher
Department of Physical Training
Krasnodar Higher Military Aviation School of Pilots
named after A.K. Serova
Russia, Krasnodar

Matsibursky Alexander Viktorovich, associate professor, senior lecturer of the department of physical training
Krasnodar Higher Military Aviation School of Pilots
named after A.K. Serova

Russia, Krasnodar

Регуляция состязательной готовности бойцов-атлетов смешанных единоборств на тренировочном этапе подготовки

Regulation of Competitive Readiness of Mixed Martial Arts Fighters-Athletes at the Training Stage of Training

Аннотация. Работа посвящена исследованию модуля проблемы релевантного управления состязательной готовностью спортсменов-рукопашников смешанных единоборств на тренировочном этапе подготовки. Методологическую и теоретическую базу работы составляли: теория адаптации (Ф. З. Меерсон, В. И. Медведев, А. В. Коробков); теория переноса тренированности (Н. А. Бернштейн и др.). Рассмотрены, в том числе, ретроспектива развития искомого контента спорта, состояние и проблемные аспекты современного рукопашного боя в системе многолетней спортивной подготовки; выявлены уязвимые звенья-модули, к которым относится недостаточный акцент тренировочного этапа на приёмы самбишенов; на основе анализа модельных характеристик действий в партере высококлассных рукопашников разработана авторская методика корригирующей тренировки. Результаты исследования показали эффективность учебно-тренировочного процесса, который осуществлялся в группах рукопашников бойцовских клубов «Спарта», «Котовск», принявших участие в эксперименте. Пять принимавших участие в составе экспериментальной группы в естественном педагогическом формирующем эксперименте спортсменов (в отличие от лиц контрольной группы) заняли призовые места на очередных «Чемпионатах России». Это эмпирическим путём подтвердило справедливость выдвинутой гипотезы работы.

Ключевые слова: спортсмены рукопашного боя, смешанные единоборства, состязательная готовность, управление, тренировочный этап подготовки, тейкдаун, самбишен.

Annotation. The work is devoted to the study of the module of the problem of relevant control of the competitive readiness of hand-to-hand athletes of mixed martial arts at the training stage of training. The methodological and theoretical basis of the work consisted of: the theory of adaptation (F. Z. Meerson, V. I. Medvedev, A. V. Korobkov); the theory of the transfer of fitness (N. A. Bernstein and others). Among other things, the retrospective of the development of the desired sports content, the state and problematic aspects of modern hand-to-hand combat in the system of long-term sports training are considered; vulnerable links-

modules are identified, which include the insufficient emphasis of the training stage on sambishen techniques; Based on the analysis of the model characteristics of actions in the referee's position of high-class hand-to-hand combatants, the author's method of corrective training was developed. The results of the study showed the effectiveness of the educational and training process, which was carried out in the groups of hand-to-hand fighters of the fight clubs "Sparta" and "Kotovsk", who took part in the experiment. Five athletes who took part in the natural pedagogical formative experiment as part of the experimental group (in contrast to the people of the control group) won prizes at the next "Russian Championships". This empirically confirmed the validity of the hypothesis of the work.

Key words: hand-to-hand combatants, mixed martial arts, competitive readiness, management, training stage, takedown, sambo.

Установлено, что важным условием продуктивности тренировочного контента по единоборствам является планирование и учет диахронической структуры парных боевых упражнений с выделением на полуобусловленные схватки и вольные бои не менее 10–15 % всего учебного времени [2, с. 48]. Однако в исследованиях недостаточно акцентируется внимание на важности контента технико-тактических действий в партере на основе принципа «силового доминирования». Анализ результативности сенсационных рейтинговых поединков ведущих бойцов смешанных единоборств (ММА), таковых, как: Хабиб Нурмагомедов, Чарльз Оливейра, Демиан Майя, Джим Миллер, Нейт Диаз, Фрэнк Мир, Ройс Грейси, Олег Тактаров, Жорж Сен-Пьер, Джон Джонс, Глейсон Тибау и др., объективно свидетельствует о действенности тейкдаунов и самбишенов преимущественно удушающими приемами.

Цель работы: изучить актуальные положения дефиниций управления состоянием состязательной готовности профессиональных бойцов-атлетов ММА на тренировочном этапе подготовки и обосновать комплексную методику повышения его эффективности.

Методика исследования. Основными методами исследования являлись: теоретический анализ и обобщение; педагогическое наблюдение; мультимедиа-визуализация; эпистемологический анализ; тестирование и контрольные испытания; проверка и оценка состязательной готовности; проверка и оценка физического состояния; моделирование и прогнозирование; педагогический эксперимент; математико-статистическая обработка результатов исследования.

Результаты исследования и их обсуждение. Актуальный ММА в системе многолетней спортивной подготовки в ходе мероприятий к рейтинговому поединку атлетов и непосредственно в ходе боя генеральным переломным

моментом соотносит «перевес» психо-эмоциогенной устойчивости бойца на фоне кумуляции кардиоваскулярно-двигательного утомления, а также уравновешенной толерантности к стресс-фактору [11, с. 340]. Это вызвано тем, что сегодня спортсмены полноценно подготовлены во всех позициях реализации их моторных кондиций в купе с тактико-техническими возможностями персонального амплуа «своих приемов». На обыденном типовом занятии спортсмен может демонстрировать титанический по интенсивности, объему, супертехническому арсеналу комплекс потенциала проявлений, тождественных достижениям мастера спорта. Однако, ударный выброс концентрированного адреналина в кровь «кора надпочечников → гипофиз», указывающий о перевозбуждении парасимпатического отдела нервной и эндокринной систем регуляции углеводного обмена, отражает имевшее место воздействие стресс-фактора, который «парализует» технико-тактическую составляющую константу бойца и демонстрирует «нисходящую зеркальную спираль» в противовес рекордам на обычной тренировке.

Актуальным аспектом современного рукопашного боя в системе многолетней спортивной подготовки является также усиление роли тактики силового доминирования [15, с. 190], представляющей инновационный подход к интеграции технико-тактической, физической и психологической подготовки атлетов. Вместе с тем в настоящее время акцент философии разумно-результативного ведения боя перераспределяется в повышение удельного веса борцовской техники [13, с. 40]. На наш взгляд, обучение защитным и атакующим действиям в партере, в целях повышения прикладного значения ММА раскрывает большие перспективы при выполнении задач в условии сложной тактической обстановки. В этой связи считаем целесообразным рассмотреть ключевые кластеры многолетней спортивной подготовки бойцов ММА. В нашей работе для эффективной координации профессиональных бойцов ММА на тренировочном этапе подготовки целесообразно применять модульно-блочный способ построения тренировочного макроцикла.

Следует подчеркнуть, что высокую роль играет «кардиоваскулярная выносливость» – работоспособность человека на фоне утомления, а также параметры «физиологической и психофизиологической стоимости реализованной физической работы (нагрузки)» [5, с. 58; 17, с. 222; 18, с. 127; 20, с. 319; 21, с. 518]. Поскольку морфо-функциональный компонент в пролонгированном многолетнем периоде видоизменяет биоструктуру тела в экономичный модельный контент реализации боя, нами исследовалось 45 спортсменов по 250 морфологическим признакам. Следует отметить, что выбор методик для оценки функционирования компонентов физического состояния спортсменов-единоборцев осуществлялся нами с учетом максимального исключения дублирования показателей, отражающих аналоговые свойства или качества того или иного параметра структуры. Это

обеспечивало релевантность получения информации о степени значимости индивидуальных показателей в структуре физического развития изучаемого контингента людей. Применением принципа «сжатия информации» и метода «просеивания» нами выявлен информативный компонент удельного веса безжировой массы тела (LBM).

Анализом техники ведения поединков на ответстсенных соревнованиях и турнирах нами установлено, что структура и многолетняя динамика соревновательной готовности высококлассных атлетов, прошедших конкурентоспособный отбор и участвующих в рейтинговых поединках, изобилует преимущественным арсеналом ударной техники. Вместе с тем мастера ММА сегодня на недостаточном уровне используют эффективные действенные тейкдауны и самбишены с акцентом на удушающую стадию, что широко используют великие единоборцы мира.

В ходе разработки модельных характеристик действий в партере высококлассных бойцов ММА нами отмечено следующее.

Анализ результативности сенсационных рейтинговых поединков ведущих бойцов смешанных единоборств объективно свидетельсивует о действенности тейкдаунов и самбишенов. Тейкдаун – это техника, которая включает в себя выведение противника из равновесия и опрокидывание его на землю, а нападающий приземляется сверху. Сабмишен – это победа с помощью удушающего или болевого приема.

Болевые и удушающие приемы – это визитная карточка ММА. Использованием метода мультимедиа-визуализации боев выдающихся мастеров смешанных единоборств, начиная с 1993 г. (UFC – 1, Ройс Грейси побеждает на турнире, причем всех своих соперников он заставил сдаться), позволило нам выявить удельный вес наиболее значимых удушающих приемов для достижения победы.

Таким образом, наиболее значимыми удушающими приёмами являются: удушение сзади и гильотина. Следовательно, процесс подготовки профессиональных бойцов ММА целесообразно усилить формированием навыков реализации вышеуказанных приёмов. Модельные биокинетические характеристики приёмов следующие.

Удушение сзади – подскочить к противнику сзади, рукой захватить голову и с одновременным ударом ногой в подколенный сгиб рвануть голову на себя; предплечьем другой руки захватить шею хватом за предплечье сверху, соединив руки и разворачиваясь влево (вправо), навалить противника себе на спину и провести удушение.

Удушающий «Гильотина» – удушающий прием, применяющийся в положениях перед и над противником. Голова противника зажимается между подмышкой и предплечьем. Атакующий ограничивает поток воздуха, поднимая предплечьем шею оппонента. Распространенное финальное удержание в смешанных боевых искусствах. Выполняется как в партере

(гард, полугард, маунт), так и в стойке. Такое название прием получил из-за визуального эффекта – при выполнении удушения не видна голова атакуемого, поэтому складывается впечатление что он без головы.

Разработка комплексной методики совершенствования финальных действий в партере у профессиональных бойцов ММА на этапе спортивной тренировки решала следующие задачи: во-первых, повышение роли психологического компонента готовности бойцов, устойчивости к воздействию эмоциогенного стресс-фактора; во-вторых, акцентированное использование бойцами средств борьбы в партере и принципиального способа «силового доминирования»; в-третьих, акцентированием внимания на финиш удушающими приемами – удушение сзади и гильотина.

Для более полного уяснения концепции нашей методики мы исходили из следующего. Во-первых, любой из 4-х этапов многолетнего совершенствования атлета предполагает наличие как минимум трех параллельных периодов: подготовительного; соревновательного; переходного или восстановительного [1, с. 35; 4, с. 197; 7, с. 20; 9, с. 42]. Во-вторых, спорт, в узком смысле своей транскрипции влияет на занимающихся посредством авто-функций. К числу их типов причисляются не только «тренирующая», «развивающая». Действенную силу также имеют функции «эмоциогенного урегулирования», «реабилитационная», «активного отдыха» [3, с. 88; 6, с. 99; 8, с. 233; 10, с. 133; 12, с. 10; 22, с. 560], которые существенно вносят своего рода прогресс-контент, ускоряя ресинтез «плохого» состояния бойца в «хорошее»; «слабого» – в «сильное»; «неудовлетворительного» – в «посредственное» или «удовлетворительное»; «неудовлетворенного» – в «удовлетворенное» (цепочку можно непрерывно продолжать по аналогии расхождения игрой дескрипторов физическое «качество» и «свойство», например, координированный – «вялый»; медленный – быстрый; твердый – мягкий; легкий – тяжелый и т. п.). Разумное варьирование тренерским штабом принципов, методов обучения и воспитания, а также гибкость форм физической подготовки с учетом сформировавшейся обстановки на данный момент для демонстрации предельно мыслимого результата, мы трактовали как концепция «оперативной избирательности» реализации эмерджентных задач участников процесса. В данной сингулярности мы находим образный аналог явления зрительно-воспринимающихся визуальных диаграмм-частот и диапазонов эквалайзера (EQ). Эти положения легли в основу нашей методики. В эксперименте участвовало 20 бойцов клубов «Котовск» и «Спарта», возраст которых составлял 19,18 ± 0,94 лет. Количество побед, поражений и ничьих ряда атлетов в профессиональном ММА соответствовало: боец «М 1» – «5–0–0»; «Н 1» – «5–1–0»; «З» – «6–0–1»; «Э» – «9–0–0»; «М 2» – «10–2–1»; «И» – «7–1–0»; «Н 2» – «8–1–1». В процессе обоснования релевантного средства, направленного на повышение стрессоустойчивости функций миокарда к

нагрузкам эмоциогенного характера, нами были разработаны правила перманентной 5-ти минутной борцовской схватки. При выигрыше болевым или удушающим приёмом, победителю начислялось 10 баллов, и бой продолжался далее в принудительном течение 5-ти минут.

При этом бойцами ЭГ тщательно отрабатывались вариации применения выявленных 2-х удушающих приемов. Интенсивность тренировок увеличивалась ступенчато [14, с. 88; 16, с. 1442; 19, с. 145]. Основными методами физической тренировки являлись сочетание повторного, интервального, соревновательного и «повторно-соревновательного» контентов. До и после педагогического эксперимента по 10 участников ЭГ и КГ (случайным отбором) были ранжированы парным сравнением и экспертной оценкой тремя опытными инструкторами по 9-ти балльному критерию их соревновательной готовности. Коэффициенты конкордации (W) с доверительным интервалом 92,0 ÷ 94,3 % соответствовали значениям 0,79 ÷ 0,89. Это подтверждало достоверность мнений экспертов. Результаты динамики соревновательной готовности бойцов отражены в табл.

Таблица

Результаты динамики соревновательной готовности бойцов в ходе педагогического формирующего эксперимента

Группы	Исходные показатели	В конце эксперимента	Достоверность различий	
	$x \pm m$	$x \pm m$	Доверительный интервал (p)	t-критерий
ЭГ	5,60±0,2	6,37±0,3	0,05	2,14
КГ	5,71±0,4	6,68±0,4	-	1,73

Из таблицы видно, что результаты ретеста бойцов ЭГ по критерию Стьюдента достоверно ($p<0,05$) превышают аналоговые значения дискриминантной группы испытуемых за счет достоверной плотности разброса параметров, отмеченных по критерию Фишера ($F = 2,1$; $p<0,05$). Идентичный показатель вариативности у КГ соответствовал: $F = 1,48$; $p>0,05$, что является своего рода психолого-педагогическим мейнстримом, поскольку в конце эксперимента абсолютные значения готовности в КГ были на 4,64% лучше. Восстановительный период исследуемых бойцов в плановом порядке трансформировался в состязательный период подготовки продолжающегося трех циклового годичного макроцикла. Пять принимавших участие в составе ЭГ в естественном педагогическом формирующем эксперименте

спортсменов (в отличие от лиц контрольной группы) выиграли очередные рейтинговые поединки классификационных боёв. Полагаем целесообразным использовать данную комбинаторику сопряженно-резонансной методики, как модуля системы управления, в практике подготовки профессиональных бойцов ММА, как компонент теории переноса тренированности в теории и методике спорта.

Выводы. Сравнительным видеоанализом поединков выявлено, что среднестатистические мастера ММА «среднего звена» сегодня на недостаточном уровне используют эффективные действенные тейкдауны и самбишены с акцентом на удушающую стадию, что широко используют великие единоборцы мира. Комплексная методика совершенствования финальных действий в партере у профессиональных бойцов ММА на этапе спортивной тренировки решала задачи: повышение роли психологического компонента готовности атлетов, устойчивости к воздействию эмоциогенного стресс-фактора; акцентированное использование средств борьбы в партере и принципиального способа «силового доминирования»; акцентированием внимания на финиш удушающими приемами – удушение сзади и гильотина.

Обоснованное релевантное средство, направленное на повышение стрессоустойчивости бойцов к нагрузкам эмоциогенного характера, заключалось в том, что при «промежуточной» победе болевым или удушающим приёмом, записывалось «+10» баллов, и бой перманентно длился 5 минут. Бои проводились в часы 72 учебно-тренировочных занятий (90 мин). Интенсивность тренировок регулировалась ступенчато. Основными методами физической тренировки являлись сочетание повторного, интервального, соревновательного и «повторно-соревновательного» контентов.

Итоги формирующего эксперимента отразили прогресс ($p<0,05$) ретеста бойцов ЭГ по критерию Стьюдента, превышающий аналоговые значения дискриминантной группы испытуемых за счет качественной плотности разброса параметров, отмеченных по критерию Фишера ($F = 2,1$; $p<0,05$). Идентичный показатель вариативности у КГ соответствовал: $F = 1,48$; $p>0,05$, что является своего рода психолого-педагогическим мейнстримом, поскольку в конце эксперимента абсолютные значения готовности в КГ были на 4,64% лучше. Восстановительный период исследуемых бойцов в плановом порядке трансформировался в состязательный период подготовки продолжающегося трех циклового годичного макроцикла. Пять принимавших участие в составе ЭГ в естественном педагогическом формирующем эксперименте спортсменов (в отличие от лиц контрольной группы) одержали уверенные победы в очередных рейтинговых поединках. Полагаем целесообразным использовать данную комбинаторику сопряженно-резонансной методики, как модуля

системы управления, в практике подготовки профессиональных бойцов ММА, как компонент теории переноса тренированности в теории и методике спорта. В целом это отразило аутентичность явления педагогического воздействия разработанной нами комплексной методики тренировки, что эмпирическим путём подтвердило справедливость выдвинутой гипотезы исследования.

Библиографический список:

1. Агабеков Н. К., Иванов Д. И., Разновская С. В. [и др.]. Критерии диагностики профессиональных компетенций обучающихся в физкультурных вузах с преимущественным учетом параметров игровых и циклических видов спорта // Гуманитарный научный вестник. 2021. № 9. С. 30—38.

2. Ашкинази С. М. Вопросы теории и практики рукопашного боя в Вооруженных Силах Российской Федерации: монография / под ред. В.Л. Марищука. СПб.: ВИФК, 2001. 240 с.

3. Горбиков И. И., Сучков В. А., Яцык В. З. [и др.]. Особенности развития специальной выносливости у лыжников в базовом мезоцикле бесснежного периода на этапе углубленной специализации // Ученые записки университета им. П.Ф. Лесгафта. 2022. № 4(206). С. 87—91.

4. Дмитриев Г. Г., Пугачев И. Ю., Щепинин В. Э. [и др.]. Модельные характеристики физической готовности выпускников военно-инженерных вузов к профессиональной деятельности // Мат-лы итог. науч. конф. института за 2003 г. СПб.: Военный институт физической культуры, 2004. С. 196—198.

5. Османов Э. М., Кораблев Ю. Ю., Пугачев И. Ю. Факторы, влияющие на эффективность физической подготовки специалистов-преподавателей старших возрастов инженерно-технических вузов министерства обороны // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2009. Т. 14, № 1. С. 57—61.

6. Пивачев А.А., Павлий А.И., Габов М.В. [и др.]. Разработка проекта Руководства по физической подготовке в Военно-Морском Флоте РФ. Отчет о НИР (Военно-морская академия), 2010. 228 с.

7. Пугачев И. Ю. Особенности организации и методики проведения учебных занятий по рукопашному бою с курсантами ВМУЗ. СПб.: Военно-морской инженерный институт, 1999. 40 с.

8. Пугачев И. Ю. Обеспечение работоспособности и формирование физической готовности специалистов инженерно-технических вузов МО РФ к профессиональной деятельности. СПб.: Нестор, 2006. 532 с.

9. Пугачев И. Ю. Интегративные научные представления о физической работоспособности обучаемых высшей школы // Интеграция образования. 2014. Т. 18, № 1(74). С. 39—46.

10. Пугачев И. Ю. Инновационная технология разработки содержания физического воспитания человека на основе принципа "сжатия информации" // Инновации в образовании. 2019. № 4. С. 130—141.

11. Пугачев И. Ю. Акцент усиления физической работоспособности военнослужащих сил специальных операций и Главного разведывательного управления РФ // Инновационные формы развития, воспитания и культуры студентов: мат-лы X международ. науч.-прак. конф. СПб.: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2020. С. 338—345.

12. Пугачев И. Ю. Научные представления о профессиональной и физической работоспособности специалиста // Kant. 2022. № 3(44). С. 4—15.

13. Пугачев И. Ю. Теоретико-методологические проблемы резонансного переноса подготовленности профессионалов ММА // ОБЖ: Основы безопасности жизни. 2022. № 5. С. 38—43.

14. Пугачев И. Ю., Блаженко С. И., Катков А. А. Профессионально-значимые физические качества специалистов в войсках противовоздушной обороны Российской Федерации // Ученые записки университета им. П.Ф. Лесгафта. 2008. № 8(42). С. 87—89.

15. Пугачев И. Ю. Кораблев Ю. Ю., Османов Э. М. Особенности профессиональной деятельности разведчиков сухопутных войск РФ и требования к их физической готовности // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2013. № 7(123). С. 188—199.

16. Пугачев И. Ю., Османов Э. М., Кораблев Ю. Ю. Проблемные положения методики обучения прикладному плаванию в Военно-Морском Флоте РФ // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2011. Т. 16, № 5. С. 1441—1449.

17. Пугачев И. Ю., Парамзин В. Б., Васильченко О. С. [и др.]. Контроль физической готовности спортсмена на различных этапах спортивной подготовки // Актуальные вопросы научно-методического обеспечения системы подготовки спортивного резерва в Российской Федерации: мат-лы Всерос. науч.-прак. конф. с междунар. уч. Казань: ФГБОУВО "Поволжская государственная академия физической культуры, спорта и туризма", 2020. С. 220—224.

18. Пугачев И. Ю., Парамзин В. Б., Разновская С. В. [и др.]. Упреждающая адаптация и перекрестная сенсибилизация в онтогенезе человека в физкультурно-образовательном пространстве // Человек. Спорт. Медицина. 2022. Т. 22, № S2. С. 124—130.

19. Пугачев И. Ю., Рубис Л. Г. Преимущественные установки использования дидактических принципов обучения в теории и методике

физического воспитания // Проблемы физической культуры, спорта и туризма в свете современных исследований и социальных процессов: сборник трудов Международ. науч.-прак. конф. СПб.: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2017. С. 143—148.

20. Разновская С. В., Васильченко О. С., Пугачев И. Ю. [и др.]. Медико-биологическое сопровождение подготовки спортсменов по смешанному стилю рукопашного боя // Ученые записки университета им. П.Ф. Лесгафта. 2021. № 7(197). С. 317—322.

21. Юрченко А. Л., Киселев А. О., Разновская С. В. [и др.]. Модернизация контента управления состоянием соревновательной готовности квалифицированных атлетов на этапе спортивного совершенствования // Ученые записки университета им. П.Ф. Лесгафта. 2022. № 10(212). С. 514—519.

22. Яцык В. З., Горбиков И. И., Васильченко О. С. [и др.]. Конкретизация тестов для оценки приоритетных физических качеств спортсменов-горнолыжников методом "просеивания" // Ученые записки университета им. П.Ф. Лесгафта. 2022. № 3(205). С. 558—563.

УДК 378

Ретивина Вероника Викторовна
старший преподаватель кафедры международного менеджмента, экономики и информационной безопасности
ФГБОУ ВО «Нижегородский государственный лингвистический университет им. Н.А. Добролюбова»,
г. Нижний Новгород, Россия

Retivina Veronika Viktorovna
Senior Lecturer at the Department of International Management, Economics and Information Security
Federal State Budgetary Educational Institution of Higher Education "Nizhny Novgorod State Linguistic University named after. ON THE. Dobrolyubova",
Nizhny Novgorod, Russia

Особенности формирования функциональной грамотности у студентов направлений высшего педагогического образования

Features of the formation of functional literacy among students of higher pedagogical education

Аннотация: В статье обосновывается важность развития функциональной грамотности у студентов педагогических направлений подготовки в связи с тем, что именно педагоги вносят значительный вклад в обучение и воспитание подрастающих поколений. Установлено, что профессиональный и компетентностный потенциал будущего педагога в первую очередь зависит от сформированного уровня функциональной грамотности. Рассмотрены особенности развития функциональной грамотности у студентов в процессе получения высшего педагогического образования. Показано, что наиболее эффективным способом для этого является комплексное использование компетентностного, личностно-ориентированного и деятельностного подходов. Выявлено, что помимо базы профессиональных знаний и интеллектуальных навыков различных видов мыслительной деятельности особо важным элементом в структуре функциональной грамотности в области педагогического образования является развитие личностных качеств будущих педагогов.
Ключевые слова: функциональная грамотность, образование, компетенции, педагогические направления подготовки.
Abstract: The article substantiates the importance of developing functional literacy among students of pedagogical training areas due to the fact that it is teachers who make a significant contribution to the education and upbringing of younger generations. It was found that the professional and competence

potential of a future teacher primarily depends on the formed level of functional literacy. The features of the development of functional literacy among students in the process of obtaining higher pedagogical education are considered. It is shown that the most effective way to do this is the integrated use of competence-based, personality-oriented and activity-based approaches. It is revealed that in addition to the base of professional knowledge and intellectual skills of various types of mental activity, a particularly important element in the structure of functional literacy in the field of pedagogical education is the development of personal qualities of future teachers.
Keywords: functional literacy, education, competencies, pedagogical directions of student training.

Актуальность изучения различных аспектов формирования функциональной грамотности будущих педагогов обусловлена исключительным значением образования для личностного и профессионального становления человека, которое должно включать в себя не только получение знаний и навыков в определенной области, но также развитие личностных качеств и способностей, которые помогут ему успешно реализоваться в выбранной профессии и быть востребованным на рынке труда.

Профессиональная успешность выпускников педагогических направлений подготовки будет будет определяться их готовностью и способностью эффективно решать возникающие в трудовой деятельности проблемы и задачи, стремлением к постоянному повышению профессионального уровня и к самореализации. Это в значительной степени зависит не только от знаний и умений, полученных в ходе обучения, но и от наличия определенных компетенций и квалификаций, которые играют ключевую роль в осознании целей современного образовательного процесса и педагогической деятельности [2, с. 219]. Важным аспектом является также обладание развитыми интеллектуальными навыками различных видов мыслительной деятельности, что, наряду с предметной компетенцией, позволяет педагогогам достигать необходимых показателей качества и эффективности своего труда. Педагогические работники должны быть готовы к ведению практиктической деятельности в динамичной, постоянно меняющейся среде, к использованию в обучении новейших технологий, передовых подходов и инновационных методик.

Ключевым результатом профессионального образования является высокий уровень образованности, формирующийся в процессе обучения и определяемый способностью человека достигать поставленных целей деятельности, сложностью и типом задач, с которыми он способен эффективно работать, базой знаний, которой он оперирует для их решения, и методами, используемыми в деятельности. Можно выделить следующие

основные уровни образованности: элементарная грамотность, функциональная грамотность и компетентность [1, с. 86].

Элементарная грамотность в контексте концепции образованности подразумевает способность к использованию базовых средств и навыков учебно-познавательной деятельности для достижения элементарных целей и решения практических задач образовательного и коммуникативного процесса. В настоящее время данный показатель тесно коррелирует с термином «образование».

Функциональная грамотность является ключевым показателем, отражающим способность человека вести эффективную трудовую деятельность. Уровень функциональной грамотности выступает в роли «индикатора» образованности индивида, который сопровождает его в течение всей жизни. Именно функциональная грамотность определяет способность личности решать стандартные и новые задачи на основе преимущественно прикладных знаний, креативно применять все приобретённые умения и навыки в различных сферах жизнедеятельности. Она включает эффективное использование межпредметных знаний, готовность к деятельности в нестабильной социальной среде и принятию ответственных решений, стремление к постоянному саморазвитию. В отличие от элементарной грамотности, функциональная грамотность является вариативным качеством, способным меняться в зависимости от различных ситуаций, и может проявляться в определенных обстоятельствах или при их изменениях, например, при смене профессиональной деятельности или образа жизни.

Компетентность обычно понимают как интеграцию основных компетенций. Компетенции рассматриваются в качестве системных образований когнитивных, аффективных и волевых качеств личности. Компетентность предполагает умение решать задачи в разных сферах жизнедеятельности на основе теоретических знаний, таких как научные теории, законы и принципы, понятия и методы науки, и практических умений и навыков личности. Ключевую роль в формировании компетентности играет уровень развития функциональной грамотности, поскольку именно она позволяет глубже и шире осмыслить знания и умения в изучаемой области.

Профессиональный и компетентностный потенциал будущего педагога также зависит от сформированного порогового уровня функциональной грамотности, отвечающего потребностям современного общества. В настоящий момент можно выделить целый ряд тенденций обественного развития, которые оказывают значительное влияние, в том числе, и на процессы образования. Среди них: повышение социальной неопределенности и рисков; цифровой и технологический скачок во всех сферах деятельности; бурный рост информационных потоков; стремление к универсализации деятельности; переход от знания к компетентности. Всё это

непосредственным образом влияет на формирование определенных требований к уровню образованности и грамотности человека, включенного в социальную жизнь и профессиональную деятельность.

Для студентов педагогических направлений подготовки формирование высокого уровня функциональной грамотности становится необходимым условием не только для личного развития, но и для успешного профессионального роста и совершенствования педагогического мастерства. Учебные программы должны учитывать современную действительность, включать в себя актуальные учебные задачи и реальные проблемные ситуации. Процесс обучения должен быть содержательным, предоставляющим студентам возможности для развития навыков, которые будут полезны во всех сферах жизнедеятельности: самостоятельность мышления, креативность, коммуникативная компетентность, широкий кругозор в общекультурной, естественнонаучной и технологической сферах и другие.

Наиболее эффективным способом развития функциональной грамотности у студентов является комплексное использование компетентностного, личностно-ориентированного и деятельностного подходов. Основная цель компетентностного подхода заключается в развитии у студентов высших учебных заведений навыков успешного решения уникальных проблемных задач, что предполагает ориентацию на личностное развитие, самосовершенствование и самореализацию. Необходимыми оказываются не только теоретические основы изучаемых учебных дисциплин, но и стимулирование самостоятельной и научной работы студентов, развитие понимания психолого-педагогических принципов организации учебного процесса и условий эффективного контроля качества профессионального образования. Переход к компетентностному подходу подразумевает формирование у преподавателей необходимых компетенций и требует создания специальной системы подготовки и переподготовки педагогических кадров [3, с. 128].

Личностно-ориентированный подход направлен на развитие личности студента, культивировании его творческой индивидуальности и интеллектуальной свободы. Его специфика основывается на важности активного участия обучающегося в образовательном процессе, и подразумевает персонализацию педагогического взаимодействия с учетом личностного опыта студента, его чувств, переживаний, эмоций. Применение такого подхода способствует развитию и закреплению профессионально- и социально-значимых качеств обучаемых, стимулированию их их творческой и социальной активности. В целом, личностно-ориентированный подход позволяет создать более гармоничную и целостную образовательную среду, где каждый студент может раскрыть свой потенциал в развитии функциональной грамотности.

Деятельностный подход ориентирован на формирование у обучающихся комплекса необходимых для будущей трудовой деятельности практических умений и навыков, а также углубленного осмысления профессиональных процессов и ситуаций. Он подразумевает активное вовлечение студентов в процесс анализа педагогических задач, "погружение" в профессиональную деятельность через различные симуляции и моделирование, а также через контекстное обучение и организацию учебно-исследовательской работы. Использование этого подхода для развития функциональной грамотности также способствует развитию профессиональной компетентности обучающихся.

В настоящее время система образования в нашей стране столкнулась с нехваткой педагогических кадров, способных обеспечить достижение превосходящих образовательных результатов обучающихся средствами определенных предметных областей, способных к гибкому и оперативному выполнению показателей качества образования, понимающих и развивающих позитивные перемены в системе отечественного образования. Вот почему развитие функциональной грамотности студентов педагогических направлений подготовки выступает предпосылкой результативности профессиональной деятельности будущих педагогов в условиях современной школы. Формирование подобных компетенций у выпускников педагогических вузов является востребованным и необходимым результатом профессиональной подготовки, удовлетворяющим требованиям современной российской школы.

Особо важным элементом в структуре функциональной грамотности в области педагогического образования является развитие личностных качеств будущих педагогов. Для того чтобы успешно справляться с профессиональными обязанностями, учителям и преподавателям необходимо завоевать уважение и доверие своих учеников, поэтому процесс развития этих качеств должен начинаться еще на этапе формирования функциональной грамотности студентов.

Личностные качества, необходимые начинающим педагогам для решения учебных и профессиональных задач, определяются в структуре всех видов функциональной грамотности, и их развитие играет важную роль в успешной трудовой деятельности. Среди наиболее важных личностных качеств педагога, которые необходимо развивать, начиная с уровня функциональной грамотности студента, можно выделить способность к эмпатии и доброжелательность, справедливость и креативность. Эмпатия дает возможность педагогу сопереживать и понимать своих учеников, а также сотрудничать с ними. Доброжелательность выражается в позитивном и доверительном отношении к обучающимся. Справедливость означает объективность и беспристрастность по отношению к ученикам. Креативность

позволяет педагогу принимать нестандартные, оригинальные решения на основе своего опыта и знаний.

Выпускники педагогических направлений подготовки сталкиваются с особенно серьезными требованиями к их квалификации, так как именно они будут нести ответственность за безопасное и комфортное взаимодействие с обучающимися не только в учебных, но и в жизненных ситуациях [2, с. 218]. Поэтому важно в процессе обучения в вузе формировать у будущих педагогов такие компетенции, которые станут основой функциональной грамотности. Для этого необходимо создать образовательную среду, способствующую развитию функциональной грамотности через моделирование различных профессиональных и жизненных ситуаций, требующих активного мышления.

Развитие и рост компетентности педагогов, призванных обеспечить подготовку кадров нового образца, высокопрофессиональных, компетентных, функционально грамотных, является необходимым условием для эффективного решение задач, стоящих сегодня перед российским обществом. Достижение технологического суверенитета нашей страны будет не только способствовать росту автономности отечественной науки и образования в ключевых сферах жизнедеятельности, но также будет работать на укрепление роли России в мировом сообществе, способствуя продвижению российских традиций, ценностей, культуры и стимулированию развития как промышленных, так и социально-гуманитарных инноваций и технологий.

Библиографический список:

1. Назарова Н.А. Развитие функциональной грамотности студентов педагогического вуза в условиях гуманитаризации образовательного процесса: специальность 13.00.08 «Теория и методика профессионального образования»: диссертация на соискание ученой степени кандидата педагогических наук / Назарова Наталья Александровна. Омск, 2007. 239 с.

2. Насырова Э.Ф., Петрова Л.В. Функциональная грамотность как одна из необходимых компетенций педагога // Мир науки, культуры, образования. 2023. № 1 (98). С. 218-220.

3. Манаенкова М. П. Компетентностный подход: от теории к практике // Преподаватель высшей школы: традиции, проблемы, перспективы: Материалы XI Всероссийской научно-практической Internet-конференции (с международным участием) , Тамбов, 26 октября 2020 года / Отв. редактор Л.Н. Макарова. Тамбов: Издательский дом "Державинский". 2020. С. 127-131.

Туракулова Мехринисо Нуриддиновна
Докторант Самаркандского государственного университета
Узбекистан, г.Самарканд

Рузикулова Нилуфар Абдумаджидовна,
кандидат биологических наук,
Доцент кафедры медицинской биологии
и генетики Самаркандского государственного медицинского университета
Узбекистан, г.Самарканд

Turakulova Mehriniso Nuriddinovna
Doctoral student of Samarkand State University
Uzbekistan, c.Samarkand

Ruzikulova Nilufar Abdumajidovna,
candidate of biological sciences,
Associate Professor of the Department of Medical Biology
and Genetics of Samarkand State Medical University
Uzbekistan, c.Samarkand

The importance of virtual laboratories in science and the types of programming used in their creation

Значение виртуальных лабораторий в науке и виды программирования, используемые при их создании

Аннотация: В статье представлена информация о виртуальных лабораториях, которые представляют собой программные продукты, их уникальных особенностях - автоматизации и эффективности проектирования, их месте в сфере образования, а также о возможности организации виртуальных лабораторий путем их изучения. Использование виртуальных комнат в образовательном процессе позволяет студентам повысить активность и самостоятельность в учебе.

Ключевые слова: виртуальная лаборатория, биология, программирование, информационные технологии, Front-End, Back-End.

Annotation: The article provides information about virtual laboratories, which are software products, their unique features are automated and design effectiveness, their place in the field of education, as well as the possibility of organizing virtual laboratories by studying them. . The use of virtual rooms in the educational process allows students to increase their activity and independence in their studies.

Key words: virtual laboratory, biology, programming, information technology, Front-End, Back-End.

It is known that in the 21st century, which is currently developing, there is no field that information technologies have not penetrated. Also, the field of education is not an exception. One of the most effective methods is the introduction and use of information technologies in education, especially in organizing lesson processes in an unconventional way. One such method is the virtual organization of laboratories.

Virtual classrooms include the design of technical objects, mathematical and simulation modeling systems, practical programs, training and production packages. An important part of a virtual instrument and a virtual laboratory is an effective graphical user interface (that is, providing a convenient, interactive mode of user interaction with a computer), a software tool with a graphical menu system in the form of graphical examples in a typical subject area is considered.

From a technological point of view, the integration of virtual laboratories into the educational process often requires the adjustment or expansion of the existing resources available in the laboratories. This is especially difficult for teachers, since they must at least understand the basic technology of virtual labs, which is usually created and implemented by highly skilled programmers and graphic designers, who must be able to introduce new content. in turn, they should cooperate with experts on relevant topics to realistically model virtual objects with their properties [6].

The educational virtual laboratory is a complete software product, the distinctive feature of which is the use of modern concepts of designing large software systems aimed at increasing the efficiency of automation and design. Methodologically, virtual laboratories can be grouped based on the types of process, declarative and hybrid systems adopted in artificial intelligence systems, based on knowledge transfer and imagination models. The basis of the practical process in the virtual educational laboratory is the educational package of practical programs or their industrial analogues. When creating them, the main attention is usually focused on mathematical modeling, optimization of the studied process or objects, and calculations. Students must have special professional qualifications in educational work with a package of practical programs. A special didactic interface, scripted

•schemes based on the following principles can help in this:

•creating competitive situations to activate learning activities;

•organization of cyclical, closed management of students' cognitive activities;

•choosing an interesting sample or teaching problem or set of problems.

The use of virtual rooms in the educational process increases the activity and independence of students in their studies, the multimedia presentation of the educational material allows to facilitate its reception, to ensure full control over the mastering of the material by each student, and to facilitate the process of preparing for exams and rating controls. Virtual labs improve student motivation, self-efficacy, and attitudes toward learning science topics. Virtual labs deserve the attention of researchers, educators, and instructional designers due to their attractive nature as a means of actively engaging students in safer and more cost-effective research. The effectiveness of virtual labs, like any other learning tool, can greatly influence how they are used in the classroom [1].

The basis of biology is practical and laboratory training. Inadequate material base is the main reason why laboratory classes are not organized at the level of demand in educational institutions. In such cases, the use of virtual laboratories helps to achieve an effective result. The relationship between educational level and virtual laboratory tools in the study of biology is very important because of the suitability of virtual laboratory tools used by students to achieve maximum learning goals.Virtual laboratories are simulations or experiments conducted on computers to present natural phenomena that play an important role in the learning process of sciences such as physics, chemistry, and biology. In other words, a virtual laboratory is a form of simulation of a real laboratory used in educational activities or scientific research to emphasize a concept or explore concepts [2]. With the development of technology, the integration of virtual experiences will definitely play a key role in shaping the future of biology education [4]. Another advantage of virtual laboratories is that they can be used to overcome the limitations associated with the high resource requirements of conventional laboratories [5].

Creating virtual laboratories requires specific knowledge, experience and time. There are several alternative software for creating virtual labs, including:

•Adobe Animate CC (or similar Adobe Flash software);

•Adobe captivate;

•Blender 3D;

•Visual coding (JAVA or other programming languages);

•Game engines [3].

One such effective program is Adobe Animate CC, which differs from other animation programs in that it provides a virtual camera function. With it, the user can easily control the movement of the camera, which gives the animation a more realistic look. For example, during the creation of a virtual laboratory, it is possible to create accurate images when moving objects from one place to another,

enlarging or reducing them. It is also possible to create 2D vector graphics of any type of line, shape, pattern, etc. through the pen functions of this program. Another feature of this program is the ability to enter text into it.

In addition, it is possible to create virtual laboratories that provide the opportunity to conduct online through the direction of creating web pages in the field of programming in information technology. Web page coding consists of two parts: Front-End and Back-End. A Front-End developer deals with the user-visible part of a website, while a Back-End developer deals with the website's database, server, and so on. It is through the study of these two areas that web pages have the opportunity to lie. Any type of web page can be created according to the discretion of the developer or customer. It is also a field of programming that has wide opportunities for creating virtual laboratories.

The basis of the guarantee of educational results is the operative response communication established in the entire educational process. The use of virtual laboratories has a special role in this. It is important to evaluate the daily results aimed at the goals of learning the educational material and to enrich the educational content.

References:

1. Byukusenge C., Nsanganwimana F., Tarmo P.A. Effectivness of virtual laboratories in teaching and learning biology: a rewiev of literature // International Journal of Learning Teaching and Educational Research. № 6. 2022. Pages 1-17.
2. Friska Damayanti Syahfitri, Binari Manurung, Muftiy Sudibyo. The Development of Problem Based Virtual Laboratory Media to Improve Science Process Skills of Students in Biology //International Journal of Research & Review. 2019. № 6. Pages 64-74.
3. Myburgh P.H. Reflecting on the creation of virtual laboratory experiences for biology students // Frontiers in education. 2022. № 7. Pages 1-9.
4. Prachi Erankar. The future of biology education: Virtual experiments revolutionize learning. India-2023. ImmersiveLabz. https://medium.com/@immersivelabz/the-future-of-biology-education-virtual-experiments-revolutionize-learning-cb3d293c3b2
5. Robert A. Desharnais, Pol Narguizian. Virtual labs for GE biology // Course redesign with technology. 2014. № 1. Pages 1-15.
6. Tiina Lynch, Ioana Ghergulescu. Review of virtual labs as the emerging technologies for teaching STEM subjects //Research and innovation. 2020. №70. Pages 6082-6091.

7. Turakulova, M., Ruzikulova, N. The significance of didactic games in assessing students'knowledge. //Science and innovation. 2023. №2(B3). Pages 65-67.

УДК 371.3

Смирнов Сергей Владимирович,
кандидат философских наук, заведующий кафедрой философии и социологии
ФГАОУ ВО «Казанский (Приволжский) федеральный университет,
Елабужский институт»
Россия, г. Елабуга

Севрюкова Софья Константиновна, студент
ФГАОУ ВО «Казанский (Приволжский) федеральный университет,
Елабужский институт»
Россия, г. Елабуга

Smirnov Sergey Vladimirovich, Candidate of Philosophy, Head of the Department of Philosophy and Sociology
Federal State Autonomous Educational Institution of Higher Education "Kazan (Volga Region) Federal University, Elabuga Institute"
Russia, Elabuga

Sevryukova Sofya Konstantinovna, student
Federal State Autonomous Educational Institution of Higher Education "Kazan (Volga Region) Federal University, Elabuga Institute"
Russia, Elabuga

Внекласная работа учителя как фактор формирования экологической культуры обучающегося

Extracurricular work of a teacher as a factor in the formation of a student's ecological culture

Аннотация. В представленной статье рассматриваются особенности внеклассной работы учителя как предпосылки формирования у школьников экологической культуры. Дается определение внеурочной деятельности, характеризуется ее дидактический потенциал и цели. Рассматриваются формы и методы организации неурочных занятий, направленных на формирование экологической культуры. Подчеркивается дидактическая значимость кружковой работы, проведения экологических конференций и игр. Акцентируется важность личной мотивации и способностей педагога как условий способствующих формированию у школьников экологической культуры. В завершении исследования делается вывод многоаспектном характере работы учителя направленной на формирование экологической культуры, зависимости данной работы от таланта педагога, ее значения как фактора организации досуга школьников, развития навыков в области охраны природы.
Ключевые слова. Экологическая культура, внеклассная работа, педагог, школьник, природа.
Annotation. The presented article examines the features of a teacher's extracurricular work as a prerequisite for the formation of an environmental culture among schoolchildren. A definition of extracurricular activities is given, its didactic potential and goals are characterized. The forms and methods of organizing extracurricular activities aimed at developing an environmental culture are considered. The didactic importance of circle work, environmental conferences and games is emphasized. The importance of the personal motivation and abilities of the teacher is emphasized as conditions contributing to the formation of an environmental culture among schoolchildren. At the end of the study, a conclusion is drawn about the multidimensional nature of the teacher's work aimed at developing an environmental culture, the dependence of this work on the teacher's talent, its importance as a factor in organizing schoolchildren's leisure time, and developing skills in the field of environmental protection.
Keywords. Ecological culture, extracurricular activities, teacher, schoolchild, nature.

Одним из приоритетных направлений работы современной школы, является развитие экологического образования как предпосылки становления у школьников экологической культуры [1].

Фундаментальные основы экологической культуры начинают закладываться в детстве. Первоочередная роль в этом процессе принадлежит

семье как важнейшему агенту первичной социализации. В тоже время, значительное место в становлении экологического мировоззрения занимает процесс обучения в общеобразовательном учреждении. Связано это с тем, что формирование экологической культуры основывается на синтезе предметных знаний из области биологии, географии, обществознания, литературы и других школьных предметов.

В соответствие с действующим ФГОС ООО, образовательная программа школы реализуется образовательным учреждением в том числе, посредством внеурочной деятельности [2]. Под ней понимают образовательную деятельность, направленную на достижение планируемых результатов освоения основной образовательной программы основного общего образования, осуществляемую в форме кружков, экскурсий, соревнований, исследований и т.д.

Внеурочная работа учителя, как фактор формирования экологической культуры, имеет огромный дидактический потенциал. Эту работу можно рассматривать как важное звено в сфере реализации дополнительного образования и воспитания, организации досуга, трудовой подготовки обучающегося, развития способностей и талантов детей в области изучения и охраны природы.

Основная цель внеклассной работы учителя в данном направлении, заключается в необходимости передачи школьникам основ знаний об окружающей среде, воспитание у них экологической бдительности, формирование практических навыков в реализации практики сбережения природы. Особую роль также имеет развитие интеллектуальных умений в сфере методологии реализации экологических исследований, конституирование экологических ценностей как совокупности ментальных качеств, основанных на представлениях о природе как базисной основе человеческого бытия [3].

Дидактические возможности внеклассной работы направленной на формирование у школьников экологической культуры, реализуются при условии ее системности и систематичности. В отсутствие этого знания учеников о природе будут иметь фрагментарный характер, а их экологическая культура основываться на реализации демонстративно-показательных мероприятий, не имеющих ни какого отношения к реализации практики реального сбережения природы [4].

Согласно А.А. Вагину, существуют следующие формы внеурочных занятий направленных на формирование у обучающихся экологической культуры [5, с. 310-311].

К ним относятся:

– обществоведческий кружок;

– поход в театр или кино;

– внеклассная экскурсия;

– организация обществоведческих конференций;

– проведение тематического школьного вечера, посвященного конкретной экологической тематике;

– организация работы школьного экологического лектория;

– организация диспутов (дебатов) на актуальные экологические проблемы;

– организация встречи школьников с представителями определенных профессий (полицейский, адвокат, экономист, социолог, судья, эколог);

– издание стенгазет и буклетов, посвященных изучению тем, связанных с экологической тематикой («глобальные проблемы человечества», «экологическое право», «структура экологических систем» и т.д.);

– проведение интеллектуальных игр;

– организация внеклассного чтения;

– подготовка проектов, рефератов по экологической тематике.

Внеурочные занятия, направленные на формирование экологической культуры можно подразделить на групповые (осуществляемые в рамках отдельного класса) и массовые (связанные с привлечением обучающихся из других образовательных организаций).

К первым относятся обществоведческий кружок, экскурсия, поход в театр или кино, создание правового уголка, организация работы школьного лектория, организация диспутов, обсуждений, организация встречи школьников с представителями определенных профессий, проведение интеллектуальных игр. Ко вторым – олимпиады, предметные конференции, дебаты среди школ города.

Большое значение во внеклассной работе учителя имеют и методы индивидуальной работы.

Индивидуальная работа связана с приобщением обучающихся к чтению и анализу экологической литературы, с выполнением экологических наблюдений и исследований.

Эти исследования могут осуществляться по таким направлениям как: климат и человек, лесной мониторинг, полевая экология, комплексный мониторинг естественных и антропогенных систем, окружающая среда и человек.

Особое значение имеет реализация кружковой работы.

При организации занятий экологического кружка необходимо подчеркивать актуальность, новизну преподаваемого материала, давать материал в доступной и интересной форме, активизировать мыслительную деятельность школьников, развивать у них игровую и творческую активность.

Не меньшее значение, имеет проведение экологических конференций и игр.

Тематикой экологических конференций может являться анализ экологических проблем конкретного города (района, Республики), способов их решения.

Экологические игры могут быть связаны с изучением жизни растений и животных; с выявлением экологических связей в экосистеме, особенностей антропогенного воздействия на биосферу, методов минимизации его последствий.

Подготовка к реализации внеурочных мероприятий направленных на формирование у школьников экологической культуры, должна опираться на формирование и развитие образовательных компетенций обучающихся, повышать интерес к изучаемому предмету, вызывать позитивные эмоции, быть личностно ориентированной.

Успех внеурочной деятельности, направленной на формирование экологической культуры во многом, зависит от желания и способностей педагога. Он должен уметь взаимодействовать с детьми зная основы детской психологии, обладать способностью мотивировать обучающихся, контролировать их самостоятельную деятельность. И т.д.

Таким образом, внеклассная работа педагога по формированию у школьников экологической культуры имеет многоаспектный характер. Реализация той или иной формы работы зависит от интересов обучающегося, умственного потенциала, интеллектуальных способностей и организационных навыков педагога. Эта работа дает возможность выбора школьниками направления и темы исследования, методов его реализации. Разнообразие форм групповой и индивидуальной работы позволяет учителю организовать их досуг, трудовую подготовку, способствует развитию навыков в области охраны природы.

Библиографический список:

1. Леонтьева И.А. К вопросу об экологизации современного школьного образования URL: https://cyberleninka.ru/article/n/k-voprosu-ob-ekologizatsii-sovremennogo-shkolnogo-obrazovaniya/viewe (дата обращения: 18.04.2023).

2. Федеральный государственный образовательный стандарт основного общего образования от 17.12.2010 г. №1897 URL: https://fgos.ru/fgos/fgos-ooo/ (дата обращения: 23.03.2023).

3. Кочарян Л.Б. Педагогические условия формирования экологической культуры младших школьников во внеклассной работе URL: https://cyberleninka.ru/article/n/pedagogicheskie-usloviya-formirovaniya-ekologicheskoy-kultury-mladshih-shkolnikov-vo-vneklassnoy-rabote (дата обращения: 12.04.2023).

4. Смирнов С.В. Эпоха экологического лицемерия // Контекст и рефлексия: философия о мире и человеке. – Т.12. – №1А. – С. 105-111.

5. Вагин А.А. Методика обучения истории в школе. – М.: Просвещение, 1972. – 351 с.

DOI 10.34755/IROK.2024.41.24.023
УДК 378.147

Стоян Геннадий Владимирович
кандидат педагогических наук, доцент кафедры "Прикладная математика"
ФГБОУ ВО "ЮРГПУ (НПИ) имени М.И.Платова"
Россия, г. Новочеркасск

Gennady Vladimirovich Stoyan, Candidate of Pedagogical Sciences,
Associate Professor of the Department of Applied Mathematics
Federal State Budgetary Educational Institution of Higher Education
"Southern State Pedagogical University (NPI) named after M.I.Platov"
Russia, Novocherkassk

Применение современных инновационных технологий в Вузах России

The use of modern innovative technologies in Russian Universities

Аннотация. В современном мире, где технологии развиваются со скоростью света, образовательные учреждения также стремятся быть на переднем крае инноваций. Вузы играют важную роль в подготовке будущих специалистов и лидеров общества, поэтому неудивительно, что они активно применяют

современные инновационные технологии для улучшения процесса обучения и достижения более высоких результатов.

Применение новейших технологий в вузах России предлагает ряд преимуществ как для студентов, так и для преподавателей. С одной стороны, использование интерактивных программ и онлайн-платформ позволяет студентам получать доступ к информации из любой точки мира, а также дает возможность изучать материалы в удобное время. С другой стороны, преподаватели могут использовать инновационные методы обучения, такие как использование виртуальной и дополненной реальности или создание интерактивных заданий, чтобы сделать учебный процесс более интересным и эффективным.

Однако применение инновационных технологий в вузах также имеет свои вызовы и ограничения. Некоторые преподаватели могут испытывать трудности в освоении новых программ или приемов, а также возникают вопросы о качестве онлайн-обучения и его способности заменить традиционные методы. Также следует учитывать финансовую составляющую - для внедрения новых технологий требуется не только обучение персонала, но и приобретение соответствующего оборудования или программного обеспечения.

Ключевые слова: инновационные технологии; онлайн-образование; качество образования; интерактивные форматы занятий.

Annotation. In today's world, where technology is advancing at the speed of light, educational institutions are also striving to be at the forefront of innovation. Universities play an important role in the training of future specialists and leaders of society, so it is not surprising that they actively use modern innovative technologies to improve the learning process and achieve better results.

The use of the latest technologies in Russian universities offers a number of advantages for both students and teachers. On the one hand, the use of interactive programs and online platforms allows students to access information from anywhere in the world, and also gives them the opportunity to study materials at a convenient time. On the other hand, teachers can use innovative teaching methods such as the use of virtual and augmented reality or the creation of interactive tasks to make the learning process more interesting and effective.

However, the use of innovative technologies in universities also has its challenges and limitations. Some teachers may have difficulty learning new programs or techniques, and questions arise about the quality of online learning and its ability to replace traditional methods. The financial component should also be taken into account - the introduction of new technologies requires not only staff training, but also the purchase of appropriate equipment or software.

Keywords: innovative technologies; online education; quality of education; interactive lesson formats.

Введение: Роль и значимость инновационных технологий в современных ВУЗах России

Современный мир стремительно развивается, и образовательные учреждения не остаются в стороне от этого процесса. В современных условиях использование инновационных технологий в высшем образовании является неотъемлемой частью успешной работы университетов. Использование таких технологий позволяет добиться ряда преимуществ как для студентов, так и для преподавателей [4].

Развитие информационных технологий играет ключевую роль в применении инноваций в ВУЗах. С помощью современного программного обеспечения и электронных платформ студенты получают возможность самостоятельного изучения материала, выполнения заданий и контроля своего академического прогресса. Преподаватели же могут использовать онлайн-курсы, видеоматериалы и интерактивные приложения для более эффективной передачи знаний. Такая форма обучения способствует повышению мотивации студентов и активному взаимодействию между преподавателями и обучаемыми.

Одной из важных инноваций, применяемых в ВУЗах, является использование виртуальной реальности. С ее помощью студенты имеют возможность погрузиться в аутентичную среду и провести эксперименты или тренировки без физического присутствия на месте. Это особенно полезно для образовательных программ, связанных с медициной, инженерией или авиации [3].

Еще одна инновация – это использование геймификации в учебном процессе. Преподаватели создают специальные игры, задания и конкурсы, которые делают обучение более интересным и захватывающим. Такой подход способствует активизации мышления студентов, развитию критического мышления и командной работы.

Также следует отметить значимость онлайн-образования в современных ВУЗах. Большое количество университетов предлагает возможность получения дистанционного образования через интернет. Это открывает новые горизонты для тех студентов, которые не могут посещать занятия в аудитории по различным причинам. Онлайн-образование также позволяет получить образование от лучших специалистов и университетов в мире, что повышает качество образования [1].

Таким образом, инновационные технологии играют существенную роль в современных ВУЗах России. Они позволяют создавать эффективную и интерактивную учебную среду, развивать навыки студентов, повышать качество образования и подготавливать выпускников к профессиональной деятельности в сфере новых технологий

Тенденции и перспективы использования инновационных технологий в образовательном процессе ВУЗов

Современные технологии непрерывно меняют нашу жизнь и вносят свой вклад в различные сферы деятельности, включая образование. ВУЗы России не остаются в стороне от этого процесса и активно применяют инновационные технологии для улучшения качества образовательного процесса.

Одной из основных тенденций использования инновационных технологий является переход к онлайн-обучению. С развитием интернет-технологий и доступности высокоскоростного интернета, все больше ВУЗов предлагает возможность получить образование дистанционно [2]. Это позволяет студентам гибко планировать свое время, избегать переезда в другой город или страну для получения образования, а также получить доступ к курсам и лекциям от ведущих специалистов со всего мира.

Еще одной перспективной технологией является использование виртуальной и дополненной реальности. Благодаря этим технологиям студенты могут буквально погрузиться в учебную среду и получить более глубокое понимание изучаемого материала. Например, в медицинском образовании студенты могут проводить виртуальные операции, а в инженерных специальностях - моделировать и тестировать различные конструкции.

Развитие информационных технологий также привело к возникновению новых методик обучения, таких как геймификация. Эта методика основана на использовании элементов игры для повышения мотивации и интереса студентов к учебному процессу. В рамках этой методики создаются учебные игры, задания с элементами соревнования и награды, что помогает студентам легче усваивать материал и активно участвовать в образовательном процессе.

Нельзя не отметить значимость использования больших данных (Big Data) в образовательном процессе [5]. Анализ больших объемов данных о поведении студентов позволяет выявлять особенности каждого конкретного студента, его проблемы или потребности. Это дает возможность персонализировать образовательный процесс и предлагать индивидуальные подходы к каждому студенту.

Таким образом, применение инновационных технологий в ВУЗах России является актуальным и перспективным направлением развития образования. Онлайн-обучение, виртуальная и дополненная реальность, геймификация и использование больших данных - все эти технологии помогают улучшить качество образовательного процесса, сделать его более интересным и доступным для студентов.

Примеры успешной реализации инновационных технологий в ВУЗах России

Примеры успешной реализации инновационных технологий в ВУЗах России в современном образовании все большее значение приобретают

инновационные технологии, которые позволяют улучшить процесс обучения и привлечь студентов к активной деятельности. Вузы России активно внедряют новаторские подходы, с целью повышения качества образования и подготовки специалистов высокого уровня.

Один из таких примеров успешной реализации инновационных технологий – использование онлайн-курсов и дистанционного обучения. Многие вузы предоставляют возможность студентам бесплатно проходить онлайн-курсы по различным предметам, что позволяет им расширить свои знания и навыки. Также многочисленные платформы для дистанционного обучения помогают студентам из любой точки страны получить доступ к качественному образованию.

Еще один пример – введение интерактивных форматов занятий. Вместо традиционных лекций и семинаров, некоторые вузы активно используют технологии виртуальной и дополненной реальности, игры и симуляции [6]. Такие занятия позволяют студентам более глубоко погрузиться в изучаемую тему, а также развивать критическое мышление и коммуникативные навыки.

Также вузы России успешно применяют инновационные технологии для оценки знаний студентов. Вместо традиционных экзаменов все чаще используются онлайн-тестирование, проектные задания, электронные портфолио. Это позволяет более объективно оценивать уровень знаний студентов и развивать их самостоятельность и творческий подход к обучению.

Одной из самых перспективных инноваций является использование искусственного интеллекта в образовании. Некоторые вузы уже начали применять системы машинного обучения для анализа данных обучения, предоставления персонализированных рекомендаций студентам, а также автоматизации некоторых аспектов учебного процесса.

Примеры успешной реализации инновационных технологий в ВУЗах России свидетельствуют о том, что современные методы обучения могут значительно повысить эффективность учебного процесса и качество образования [1]. Однако для полноценного внедрения и использования инноваций необходимо подготовить соответствующую инфраструктуру, обучить преподавателей новым методам работы и создать условия для активного взаимодействия студентов с инновационными технологиями

Преимущества и вызовы при внедрении инновационных технологий в ВУЗы России

Применение современных инновационных технологий в вузах России имеет свои преимущества и вызовы. В данном подразделе рассмотрим основные аспекты этого процесса.

Одним из главных преимуществ использования инновационных технологий в высшем образовании является повышение качества обучения. Использование интерактивных электронных платформ, онлайн-курсов и

мультимедийного контента помогает сделать учебный процесс более интересным и доступным для студентов. Они могут самостоятельно изучать материал, задавать вопросы и получать обратную связь от преподавателей. Это способствует более глубокому усвоению знаний и развитию навыков самостоятельной работы.

Еще одним преимуществом является расширение возможностей для научно-исследовательской работы студентов. Благодаря инновационным технологиям они могут проводить эксперименты, моделирование и анализировать данные с помощью специализированного программного обеспечения [6]. Это способствует развитию их аналитических навыков, креативности и инновационного мышления.

Однако внедрение инновационных технологий также представляет вызовы для вузов. Во-первых, требуется значительные финансовые затраты на приобретение необходимого оборудования, программного обеспечения и подготовку персонала. Не все вузы могут себе позволить эти расходы.

Во-вторых, для успешного внедрения инноваций необходима поддержка со стороны администрации и преподавательского состава. Некоторые преподаватели могут испытывать сопротивление по отношению к новым технологиям из-за незнания или неприятия изменений в учебном процессе. Поэтому необходимо проводить систематическую работу по информированию и обучению преподавателей о преимуществах использования инновационных технологий.

Также следует учитывать потенциальные риски, связанные с безопасностью данных и конфиденциальностью личной информации студентов. Важно создать соответствующие механизмы и политику по защите данных, чтобы предотвратить возможные утечки или злоупотребления.

Тем не менее, преимущества использования инновационных технологий в вузах России перевешивают вызовы. Они позволяют повысить качество образования, развить научно-исследовательский потенциал студентов и подготовить их к требованиям современного рынка труда. Поэтому важно продолжать активное внедрение и поддержку инновационных технологий в высшем образовании страны.

Рекомендации по эффективному использованию инновационных технологий в ВУЗах России

В последние годы применение современных инновационных технологий в высшем образовании стало неотъемлемой частью образовательного процесса. Однако, для эффективного использования этих технологий в ВУЗах России необходимо учитывать ряд особенностей и следовать определенным рекомендациям.

Первая рекомендация связана с выбором подходящих инновационных технологий. ВУЗы должны анализировать текущие требования и потребности

студентов, а также оценивать возможности новых технологий. Например, использование онлайн-платформ и мобильных приложений может значительно облегчить доступ к учебной информации и создать интерактивные формы обучения.

Вторая рекомендация связана с подготовкой преподавателей. ВУЗы должны предоставлять возможности для повышения квалификации преподавателей по вопросам применения инновационных технологий. Это поможет им осуществлять более эффективное использование этих технологий в своей практике и успешно взаимодействовать с современным поколением студентов.

Третья рекомендация связана с созданием подходящей инфраструктуры. ВУЗы должны обеспечивать доступ к высокоскоростному интернету, обновлять компьютерное оборудование и оснащать аудитории новейшей техникой. Также необходимо разработать удобные и интуитивно понятные интерфейсы для использования инновационных технологий.

Четвертая рекомендация связана с постоянной оценкой и анализом результатов. ВУЗы должны проводить систематический мониторинг эффективности использования инновационных технологий и адаптировать свои методики на основе полученных данных. Это поможет определить успешные практики, а также выявить проблемные места, требующие дальнейшего усовершенствования.

Пятая рекомендация связана с активной работой над развитием цифровой грамотности студентов. ВУЗы должны предоставлять возможности для приобретения навыков работы с новыми технологиями и информационными ресурсами. Это поможет студентам быть конкурентоспособными на рынке труда и успешно применять полученные навыки в своей будущей профессиональной деятельности.

В заключение, эффективное использование инновационных технологий в ВУЗах России требует комплексного подхода. Необходимо выбирать подходящие технологии, обучать преподавателей, создавать соответствующую инфраструктуру, анализировать результаты и развивать цифровую грамотность студентов [2, 4].

Библиографический список:

1. Березина Е.Н., Морозова Н.Г., Шадриков В.Д. Инновационные процессы в образовании: проблемы и перспективы. – М.: Издательство "Наука", 2022.

2. Министерство науки и высшего образования Российской Федерации. Стратегия инновационного развития Российской Федерации на период до 2030 года. – М., 2020.

3. Смирнова З.В., Чистякова Г.П. Инновации в системе высшего образования: опыт и проблемы. – М.: Издательство "Перспектива", 2021.

4. Федоров А.А., Ахметзянова Л.С. Инновационные технологии в образовании: педагогика нового времени. – М.: Издательство "Академия", 2020.

5. Цифровая трансформация образования в России: аналитический доклад. – М.: Национальный исследовательский университет "Высшая школа экономики", 2022.

6. Шевцова Е.Г., Шестакова Л.В. Инновационные методы обучения в высшем образовании. – М.: Издательство "Флинта", 2021.

Социологические науки

DOI 10.34755/IROK.2024.75.36.024
УДК 101.2

Кузёмина Елена Фёдоровна
канд. филос. наук., доц.каф.
«История, философия и психология»
ФГБОУ ВО «Кубанский государственный технологический университет»
Россия, г. Краснодар

Щербаков Иван Сергеевич, студент кафедры
«Теплоэнергетика и теплотехника»
ФГБОУ ВО «Кубанский государственный технологический университет»
Россия, г. Краснодар

Kuzyomina Elena Fedorovna, Ph.D. Philosopher Sci., Assoc. Dept.
"History, philosophy and psychology"
Federal State Budgetary Educational Institution of Higher Education "Kuban State Technological University"
Russia, Krasnodar

Shcherbakov Ivan Sergeevich, student of the department

“Thermal power engineering and heating engineering”
Federal State Budgetary Educational Institution of Higher Education "Kuban State Technological University"
Russia, Krasnodar

Современное понимание интуиции в познавательном процессе и творчестве

Modern understanding of intuition in the cognitive process and creativity

Аннотация. В статье рассматривается влияния интуиции, продуктивного воображения и формализованных доказательств на познавательный процесс и творчество. Анализируется взаимосвязь этих элементов и их роль в различных областях человеческой деятельности. Интуиция, как неформальный механизм восприятия, взаимодействует с формализованными методами, дополняет их и предоставляет обширные возможности для понимания многообразных явлений. Продуктивное воображение, в свою очередь, стимулирует творческий процесс, генерируя оригинальные идеи и концепции. Современное понимание интуиции представляется как комплексный и сложный процесс, включающий неосознаваемые источники информации, скрытые ассоциации, инновационные идеи и нестандартные решения. Сочетание этих элементов создает новые перспективы в науке, искусстве и бизнесе, что делает их важными объектами для исследования.
Ключевые слова: иинтуиция, воображение, продуктивность, творчество, формализация, абстракция, решения, познание, анализ.
Annotation: The article examines the effects of intuition, productive imagination and formalized evidence on the cognitive process and creativity. The interrelation of these elements and their role in various fields of human activity is analyzed. Intuition, as an informal mechanism of perception, interacts with formalized methods, complements them and provides extensive opportunities for understanding diverse phenomena. Productive imagination, in turn, stimulates the creative process by generating original ideas and concepts. The modern understanding of intuition is presented as a complex and complex process, including unconscious sources of information, hidden associations, innovative ideas and non-standard solutions. The combination of these elements creates new perspectives in science, art and business, which makes them important objects for research.
Keywords: intuition, imagination, productivity, creativity, formalization, abstraction, solutions, cognition, analysis.

Интуиция, эта загадочная и в то же время важная составляющая человеческой психики, продолжает привлекать внимание ученых различных областей знания. Ее сложность и многогранность стимулируют исследователей к поиску новых подходов к пониманию этого явления. Рассматривая современное понимание интуиции и ее связь с формализованными типами доказательств, видами интуитивного творчества и продуктивным воображением раскрывается ее неисчерпаемый познавательный потенциал [1].

Начнем с общего понимания интуиции. Интуиция – это нечто большее, чем просто инстинктивное чувство или предчувствие. Она позволяет считывать бессознательную информацию и делать быстрые выводы без осознанного анализа. Например, когда мы встречаем нового человека и немедленно ощущаем, нравится ли нам он или нет, это проявление интуиции [2,3].

Цель нашего исследования заключается в попытке разобраться в том, как интуиция взаимодействует с формализованными типами доказательств и как она проявляется в различных видах творчества. Разбираясь в этом, мы сможем лучше понять роль интуиции в познавательном процессе и ее значение для нашей повседневной жизни.

Характеристики интуиции включают в себя способность оперативного распознавания ситуаций, где логическое мышление может быть ограничено. Например, врачи, имея богатый опыт, могут, опираясь на интуицию, быстро выделить важные аспекты заболевания пациента, даже если симптомы неоднозначны [2, 4].

Интуиция играет значительную роль в познавательном процессе, обогащая его и обеспечивая дополнительные аспекты восприятия мира. Она дополняет формальные методы доказательства, предоставляя быстрый и неосознанный доступ к информации, что особенно ценно в ситуациях временного дефицита.

Проявляясь в моменты принятия решений, интуиция способствует выделению ключевых факторов и формирует индивидуальный взгляд на проблему. Это проявляется в профессиональной деятельности, например, у опытных менеджеров, которые, оперируя интуитивно, могут принимать стратегические решения, основанные на неформальных оценках ситуации. Таким образом, интуиция дополняет логический аспект познания, предоставляя более полное и гибкое понимание окружающего мира.

Механизм интуитивного восприятия тесно взаимодействует с формализованными типами доказательств, обогащая их и предоставляя дополнительные информационные слои [4]. Интуиция выступает в роли неформального фильтра, пропускающего через себя контекстуальные аспекты и смысловые нюансы, которые могли бы остаться невидимыми для строго формальных методов.

Применительно к научным исследованиям, интуитивные инсайты могут помочь в поиске неожиданных связей в данных, указывая на потенциальные тенденции или важные аномалии [4]. Например, в области математики, где формализованные доказательства играют ключевую роль, интуиция математика может подсказать направление поиска решения, даже если строгие логические шаги еще не ясны. Интуиция также может служить критическим фактором в процессе формализации доказательств, помогая исследователям выявить неявные предположения или лакуны в логической цепи. Таким образом, взаимодействие интуиции с формальными методами доказательства создает динамичное и взаимовыгодное партнерство, обеспечивая комплексный и более глубокий анализ данных и явлений.

В рамках психологического контекста, сублиминальное восприятие, как механизм, предшествующий интуитивным абстракциям, представляет собой бессознательное восприятие внешних стимулов, проникающее в сознание ниже порога осознания. На уровне абстракции, это явление проявляется в формировании неявных, недоступных логическому разбору концепций и идей. Примером сублиминального восприятия может служить сценарий, когда человек, не осознавая полностью визуальные детали, интуитивно улавливает эмоциональную окраску и общую суть изображения. Это, в свою очередь, может послужить основой для дальнейших интуитивных абстракций, когда бессознательно формируются обобщенные представления об объекте или явлении.

Интуитивное принятие решений тесно связано с творческим процессом, где индивидуальная интуиция выступает в качестве ключевого компонента. В контексте творчества, интуитивное решение означает быстрый и бессознательный выбор, основанный на неформальном анализе ситуации и индивидуальном опыте [3, 4]. Примером может служить творческий акт художника, который, ориентируясь на интуитивные внутренние представления, создает произведение искусства. Этот творческий процесс подчеркивает роль интуитивного принятия решений в формировании новаторских идей и выражении индивидуального творческого стиля. Таким образом, интуитивное принятие решений становится неотъемлемой составляющей творческого акта, обогащая его оригинальностью и глубиной выражения.

Продуктивное воображение, как часть творческого процесса, эффективно воздействует на интуитивное творчество, создавая гармоничные образы и стимулируя новые идеи. Например, в творчестве художника оно может влиять на сочетания цветов, а в научных исследованиях подсказывать интуитивные гипотезы. Таким образом, продуктивное воображение действует как катализатор для интуитивного творчества, открывая путь к нестандартным идеям.

В итоге, анализ взаимодействия интуиции, продуктивного воображения и формализованных доказательств подчеркивает их значимость в познавательном процессе и творчестве. Интуиция дополняет формальные методы, а продуктивное воображение стимулирует творческий поток. Этот симбиоз открывает новые перспективы в науке, искусстве и бизнесе, подчеркивая уникальность каждого элемента. Наше исследование призывает к дальнейшему изучению этой взаимосвязи для более эффективного решения сложных задач.

Библиографический список:

1. Куземина Е.Ф., Пашкова Н.В., Басманова В.Р. Интуитивное знание как важнейшая сфера человеческого познания // Сборник материалов VII Международной научно-практической очно-заочной конференции Филологические и социокультурные вопросы науки и образования. Краснодар, 2022. С. 979-984.
2. Китаева, И. Ю. Из истории понимания интуиции в философии / И. Ю. Китаева // Социально-гуманитарный вестник : Всероссийский сборник научных трудов. Том Выпуск 25. – Краснодар : Краснодарский центр научно-технической информации, 2019. – С. 8-12. – EDN BKCTTE. URL: https://www.elibrary.ru/item.asp?id=41433512 (дата обращения: 10.02.2024)
3. Бондаренко, А. В. Интуиция и творчество / А. В. Бондаренко // Историческая и социально-образовательная мысль. – 2014. – Т. 6, № 6-2. – С. 50-54. – EDN TIXLKN. URL: https://www.elibrary.ru/item.asp?id=31740466&pff=1 (дата обращения: 10.02.2024)
4. Федосеенков, А. В. Роль воображения и интуиции в познавательном процессе / А. В. Федосеенков, В. А. Ермилова, И. Ю. Местоев // Наука молодых - будущее России : Сборник научных статей 2-й Международной научной конференции перспективных разработок молодых ученых. В 5-ти томах, Курск, 13–14 декабря 2017 года / Ответственный редактор А.А. Горохов. Том 2. – Курск: Закрытое акционерное общество "Университетская книга", 2017. – С. 319-322. – EDN YBDCEJ. URL: https://www.elibrary.ru/item.asp?id=22981391 (дата обращения: 10.02.2024)

DOI 10.34755/IROK.2024.30.65.025

Семешин Павел Юрьевич
Студент 2 курса магистратуры РГСУ
направления подготовки «Социология»
очной формы обучения

Semeshin Pavel Yurievich
2nd year master's student at RGSU
areas of training "Sociology"
full-time education

Любительские турниры по настольному теннису как способ поддержания мотивации к занятиям спортом
Amateur table tennis tournaments as a way to maintain motivation for sports

Аннотация: Данная статья рассматривает способы поддержания мотивации к занятиям спортом у жителей РФ (в частности настольным теннисом). Особое внимание уделяется продвижению настольного тенниса. Изучаются причины низкой популярности данного вида спорта в России, даются предложения по работе над улучшением сложившейся ситуации. Изучаются данные двух социологических исследований, проведенных автором статьи, а

также рекомендации Президента Российской Федерации Владимира Владимировича Путина.
Ключевые слова: настольный теннис, спорт, турниры, состязания, конкуренция, мотивирование, мотивация, продвижение, лидеры мнений, спортивная психология.
Annotation: This article examines the ways to maintain motivation for sport activities among residents of the Russian Federation (table tennis players as well). Much attention is paid to the promotion of the table tennis. The reasons for the low popularity of this sport in Russia are studied, and proposals are given for working to solve this problem. The data of two sociological studies conducted by the author of the article is the core of the analysis, as well as the recommendations of the President of the Russian Federation Vladimir Vladimirovich Putin.
Key words: table tennis, sports, tournaments, competitions, competition, motivation, motivation, promotion, opinion leaders, sports psychology.

В эпоху возрастающей роли интернета в жизни и работе людей, а также повышения уровня так называемой цифровой интоксикации крайне важно мотивировать население уделять внимание своему здоровью и заниматься спортом. По данным ВЦИОМ (Всероссийский центр изучения общественного мнения), граждане Российской Федерации стали чаще приобщаться к спорту. Сегодня 54% россиян регулярно уделяют внимание физическим нагрузкам и занимаются спортом 1-3 раза в месяц и чаще, в том числе 18% занимаются спортом на ежедневной основе. 22% жителей РФ посвящают время физической активности не реже 2-3 раз в неделю. [1]

Активно способствует популяризации спорта и мнение Президента Российской Федерации Владимира Владимировича Путина. На заседании Совета по физкультуре и спорту в 2023 г. глава государства отметил, что продвижением спорта надо заниматься «активно» [4]. Активное продвижение различных видов спорта сейчас можно наблюдать во всей стране. Также президента удивило практически полное отсутствие у россиян интереса к настольному теннису.

Повышение интереса к настольному теннису - важная задача для страны. Во-первых, этот вид спорта можно назвать относительно дешевым. Экипировка стоит в разы меньше, чем форма и необходимые приспособления для многих других видов спорта. Во-вторых, настольный теннис дает отличную нагрузку на весь организм. Эта динамичная игра позволяет получить необходимую кардионагрузку, укрепить мышцы, развить опорно-двигательный аппарат, улучшить координацию и скорость реакции. В-третьих, компактные столы для настольного тенниса можно установить в большинстве дворов российских городов. Это не потребует таких затрат, как, например, создание скалодромов или залитие катков.

На данном этапе многие эксперты сходятся во мнении, что низкая популярность настольного тенниса связана с недостаточной популяризацией этого вида спорта. Осенью 2023-го года автор данной статьи провел социологическое исследование в форме онлайн-анкетирования на платформе CreateSurvey [6] с целью выявления причин, по которым люди выбирают другие виды спорта. Всего в опросе приняли участие 200 респондентов в возрасте от 18 до 60 лет. Соотношение лиц обоих полов было равным. Также на этапе отбора респондентов были отсеяны все те, кто вообще не занимается спортом. Отсев происходил при помощи системы ветвлений на платформе проведения опроса [2]. Большинство респондентов (79%) сообщили, что при выборе вида спорта они вообще не рассматривали настольный теннис. 23% респондентов при этом сказали, что даже не вспомнили об этом виде спорта. Отдельный интерес представили люди, которые пробовали заниматься настольным теннисом, но потом сменили вид спорта. Как оказалось, большинству их них стало неинтересно в связи с отсутствием мотивации в виде соревнований и интереса общественности.

В сложившейся ситуации можно предложить два основных пути популяризации настольного тенниса:

1. Активное и креативное продвижение этого вида спорта.
2. Поддержание мотивирования у тех, кто уже занимается настольным теннисом.

Важно отметить, что в обоих случаях речь идет о продвижении вида спорта среди любителей, а не профессионалов, так как у профессиональных спортсменов принципиально иная мотивация.

Для популяризации настольного тенниса можно использовать возможности интернета, социальных сетей и лидеров мнений. Так, например, привлечение блогеров может дать ощутимые результаты. По данным исследования, проведенного в 2022 г. совместными силами ВЦИОМ и продюсерского центра Insight People, россияне стали больше доверять блогерам. Сегодня каждый пятый житель РФ прислушивается к мнению блогеров, а более трети россиян на регулярной основе пользуются социальными сетями и черпают информацию из них. [5]

Для поддержания мотивации занимающихся любителей необходимо создать атмосферу азарта и конкуренции. Именно это в спорте стимулирует людей прикладывать больше усилий к победе. Это отметил и Президент Российской Федерации. Владимир Владимирович сообщил, что в России запланировано значительное увеличение количества спортивных соревнований разного уровня [3]. Речь идет и о любительских турнирах.

И если профессиональные спортсмены имеют возможность участвовать в соревнованиях на региональном, федеральном или международном уровнях, то любители часто лишены такой возможности и ограничиваются обычной

игрой с друзьями, что не способствует мотивированию к более активным занятиям.

Отличным решением может стать проведение любительских турниров настольного тенниса, которые сегодня есть в РФ, но в недостаточном количестве и без должного освещения. Прекрасным примером любительских турниров могут стать состязания, о которых сообщает RTTF (Russian table tennis forum) - российский форум настольного тенниса.[7] На форуме аккумулируется информация о любительских соревнованиях, в которых могут принять участие игроки разного уровня. Каждый игрок получает определенные баллы рейтинга и в зависимости от этих баллов может выбрать себе подходящий турнир. Таким образом, на состязании подбираются соперники примерно одинакового уровня, что делает игру интересной. Кроме того, за победу на турнире предусмотрены призы. Призы меняются в зависимости от уровня состязания и от желаний организаторов турнира.

Для того, чтобы понять, насколько подобные турниры мотивируют игроков продолжать занятия настольным теннисом, автором статьи было проведено социологические исследования в формате фокус-группы. Были опрошены участники RTTF, которые регулярно участвуют в турнирах.

Во время проведения фокус-групповой дискуссии респонденты сообщили, что им нравится участвовать в состязаниях из-за здоровой конкуренции. Это главный стимул, который выделили все респонденты. Также крайне важным оказалась возможность найти соперников своего уровня. Респонденты отметили, что игра с друзьями быстро надоедает, так как уровень подготовки очень сильно разнится. В связи с этим одному из участников приходится либо играть в полсилы, либо вообще использовать неведущую руку, чтобы хоть как-то уравнять возможности. Третьим по важности моментом для игроков стала возможность играть в настольный теннис без необходимости самостоятельно организовывать встречи. Если при игре с друзьями часто приходится бронировать зал, согласовывать время и заниматься другими вопросами менеджмента, то турниры избавляют от лишних забот. И, конечно, в качестве четвертого важного мотивирующего фактора респонденты назвали наличие призов. При этом материальная ценность приза, как оказалось, играет второстепенную роль, а главным для игроков становятся сами эмоции при получения приза. Наиболее приятными призами игроки назвали медали и кубки. Респонденты отметили, что после начала участия в турнирах стали намного больше заниматься спортом, охотнее посещать тренировки и соревнования. Кроме того, смогли привлечь к спорту своих родных и знакомых, что способствует популяризации спорта в целом и настольного тенниса в частности.

Такие результаты исследования в очередной раз подтверждают мнение психологов, которые отмечают пользу конкуренции в спорте. При здоровой конкуренции спортсмен (как профессионал, так и любитель) может легче

проявить скрытые резервы организма. Также усиливается стрессоустойчивость и воля к победе. И, главное, повышается мотивация и усиливается желание заниматься спортом.

Часто профессиональные тренеры, которые обучают не только профессиональных игроков, но и любителей, рекомендуют ученикам время от времени пробовать свои силы в любительских турнирах.

Психологи часто называют соперничество главным мотивационным ресурсом. Именно этот ресурс дает спортсменам участие в турнирах и состязаниях.

Результаты проведенных исследований, а также мнения специалистов наглядно демонстрируют значимость любительских турниров для поддержания мотивации к занятиям спортом у игроков-любителей. Грамотная организация состязаний может стать отличным способом продвижения настольного тенниса в массы и популяризации данного вида спорта среди населения Российской Федерации.

Библиографический список:

1. ВЦИОМ. Результаты мониторингового опроса на тему спорта. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/sport-dlja-vsekh (дата обращения — 15.02.24)
2. Иванова В. А. Исследования в маркетинге и рекламе. Учебное пособие, РАНХиГС, 2021.
3. Известия. Официальный сайт. URL: https://iz.ru/1592133/2023-10-19/putina-udivilo-otsutstvie-u-rossiian-interesa-k-nastolnomu-tennisu (дата обращения — 17.02.24)
4. Тасс. Путин считает важным красиво и креативно популяризировать разные виды спорта. URL: https://tass.ru/sport/19063963 (дата обращения — 11.02.24)
5. Отчет об исследовании ВЦИОМ и Insight People. URL: https://incrussia.ru/pnews/research-insight-people/ (дата обращения — 17.02.24)
6. Тюрин И. Н. Проведение социологического опроса с помощью CreateSurvey. Статья. URL: https://www.createsurvey.ru/papers/make-socium-survey-with-createsurvey.htm (дата обращения — 22.11.23)
7. RTTF. Официальный сайт российского форума по настольному теннису. URL: https://rttf.ru/ (дата обращения — 24.01.24)

Экономические науки

УДК 64.011.32

Аблитаров Э.Р., Белялов А.А.
обучающиеся направления подготовки 38.03.01 «Экономика», гр. Э-б-о-205
Институт экономики и управления ФГАОУ ВО
«КФУ им. В.И. Вернадского»
г. Симферополь, Россия

Шамилева Э.Э.
Научный руководитель, к.э.н., доцент кафедры экономики предприятия
Институт экономики и управления ФГАОУ ВО
«КФУ им. В.И. Вернадского»
г. Симферополь, Россия

Ablitarov E.R., Belyalov A.A.
students in the training area 03/38/01 "Economics", gr. E-b-o-205

Institute of Economics and Management of the Federal State Autonomous Educational Institution of Higher Education "KFU im. IN AND. Vernadsky" Simferopol, Russia

Shamileva E.E.
Scientific supervisor, Ph.D. in Economics, Associate Professor of the Department of Enterprise Economics
Institute of Economics and Management of the Federal State Autonomous Educational Institution of Higher Education "KFU im. IN AND. Vernadsky" Simferopol, Russia

АНАЛИЗ ЗАПАСОВ МАТЕРИАЛЬНЫХ РЕСУРСОВ И ЭФФЕКТИВНОСТЬ ИХ ИСПОЛЬЗОВАНИЯ

ANALYSIS OF STOCKS OF MATERIAL RESOURCES AND THE EFFECTIVENESS OF THEIR USE

Аннотация. В работе проведен анализ запасов материальных ресурсов и оценена их эффективность использования на предприятии. Изучены теоретические и методологические аспекты анализа запасов, рассмотрено их влияние на непрерывность и эффективность производственного процесса. Предложены методики для оптимизации использования материальных ресурсов, способствующие улучшению операционной эффективности и повышению прибыльности предприятий.

Ключевые слова: запасы материальных ресурсов, анализ эффективности использования, управление запасами, оптимизация ресурсов, производственный процесс, экономическая эффективность.

Annotation. The article analyzes the reserves of material resources and evaluates their efficiency of use in the enterprise. The theoretical and methodological aspects of stock analysis are studied, their impact on the continuity and efficiency of the production process is considered. The methods for optimizing the use of material resources are proposed, which contribute to improving operational efficiency and increasing the profitability of enterprises.

Key words: inventories of material resources, analysis of efficiency of use, inventory management, resource optimization, production process, economic efficiency.

На современном этапе экономических отношений развитие любого государства неразрывно связано с функционированием корпоративного сектора, основой успешной деятельности которого является обеспечение

непрерывности и эффективности производственного процесса. Посредством использования запасов материальных ресурсов решаются важные стратегические задачи, включая создание и поддержание товарного ассортимента на должном уровне для удовлетворения спроса потребителей. В этой связи, анализ запасов материальных ресурсов играет значимую роль, определяя пропорции различных категорий товаров и материалов, которые предприятие использует для поддержания производственного процесса. В свою очередь, эффективность использования запасов материальных ресурсов выступает ключевым индикатором для расчета экономической выгоды от использования имеющихся ресурсов, отражая издержки, связанные с хранением и транспортировкой ресурсов.

Целью работы является изучение теоретико-методических и методологических аспектов проведения анализа запасов материальных ресурсов предприятия. Для этого следует изучить экономическое содержание, виды и роль запасов материальных ресурсов, а также исследовать методику анализа данной категории.

Одним из условий обеспечения непрерывности и эффективности производственного процесса является наличие и использование запасов материальных ресурсов, следовательно, при организации любого процесса производства актуализируется проблематика эффективности их использования как составляющей эффективности деятельности предприятия. Под данной экономической категорией понимают совокупность материалов, сырья, полуфабрикатов, готовой продукции и других материальных активов, которые находятся в собственности предприятия и предназначены для использования в процессе производства товаров и услуг, для продажи или для поддержания текущей деятельности [1, с. 215]. На рисунке 1 представлены основные характеристики запасов материальных ресурсов предприятия.

Рисунок 1 – Основные характеристики запасов материальных ресурсов предприятия

Источник: составлено автором на основе [1, с. 215-217]

Исходя из рисунка 1, выделяют три основные категории, на которые можно классифицировать запасы материальных ресурсов предприятия. В первую категорию входят ресурсы, используемые в качестве сырья или материалов в производстве продукции или при оказании услуг (природные ресурсы, покупные полуфабрикаты). Вторая категория охватывает готовую продукцию и товары, предназначенные для продажи. Третья категория представляет собой ресурсы, используемые для управленческих нужд предприятия, включая материалы, топливо, запасные части и др. Такое понятийно-категориальное разделение позволяет лучше понять и управлять запасами предприятия, оптимизируя использование каждой категории в соответствии со стратегическими целями организации.

Из этого следует, что в деятельности предприятий запасы материальных ресурсов обеспечивают непрерывность производственной и сбытовой деятельности: сглаживание непредвиденных колебаний спроса, сбоев в поставках и операционной деятельности, повышение надежности логистики. Исходя из вышеизложенного, превышение запасов влечет дополнительные затраты на хранение и налоги, тогда как недостаток может привести к задержкам в производстве. В связи с этим, своевременный анализ запасов материальных ресурсов является ключевым для поддержания эффективности деятельности предприятия.

Основную информационную базу экономического анализа использования материалов составляют данные бухгалтерской и финансовой отчетности, плановые и отчётные калькуляции себестоимости продукции, материалы плановых, финансовых служб, а также технологических, конструкторских и других функциональных подразделений предприятия (цехов, участков), которые обязаны принимать непосредственное участие в организации бесперебойного снабжения предприятия всеми необходимыми материальными ресурсами и в поиске резервов экономии этих ресурсов [2, с. 55].

Отсюда следует, что анализ запасов материальных ресурсов предприятия основывается на научно-обоснованных методиках и учитывает специфику деятельности предприятия. При реализации таких методик включают взаимосвязанные этапы для обеспечения полноты и достоверности получаемой информации. Рассмотрим последовательность этапов анализа запасов материальных ресурсов [3, с. 154]:

1. анализ тенденций изменения запасов материальных ресурсов является важным на начальном этапе, поскольку ряд показателей на последующих этапах требуют оценки показателей в динамике и установления нормативов за предыдущие периоды анализа;

2) оценка состава и структуры запасов материальных ресурсов осуществляется путем сравнения фактических показателей с нормативными базами сравнения; результаты оценки могут определить удельный вес

запасов в общем объеме ресурсов или долю запасов в общей сумме оборотного капитала предприятия;

3) эффективность использования запасов материальных ресурсов предприятия оценивается с помощью показателей: материалоёмкость продукции, материалоотдача, удельный вес материальных расходов в себестоимости продукции и т.д.;

4) факторный анализ производится для определения степени влияния исследуемых факторов на уровень остатков и движение материальных запасов, что позволяет выявить, какие факторы оказывают наибольшее положительное и негативное воздействие на уровень и использование запасов, и разработать стратегии для нивелирования проблемных областей;

5) выявление излишков производственных запасов позволяет сократить издержки и повысить производительность, что приводит к повышению ликвидности предприятия.

Для оценки необходимого объема запасов материальных ресурсов для деятельности предприятия используется показатель оборачиваемости запасов (Поз). Показатель рассчитывается по следующей формуле (1):

$$\text{Поз} = \frac{\text{Ч}}{\text{З}} \quad (1)$$

где Поз – оборачиваемость запасов;

Ч - чистый объем реализации;

З – стоимость запасов на начало периода.

Высокое значение показателя оборачиваемости запасов свидетельствует о способности предприятия быстро превращать запасы в продукцию, а затем в денежные средства. Низкое значение показателя, напротив, указывает на недостаточную эффективность управления запасами и возможные проблемы с ликвидностью, что может быть вызвано избыточными запасами, недостаточной скоростью оборота товаров, низкой спросом на продукцию или проблемами в цепочке поставок.

Продолжительность одного оборота запасов определяется как период, за который запасы полностью оборачиваются, и вычисляется по формуле (2):

$$\text{Пр. оз} = \frac{\text{П}}{\text{Поз}} \quad (2)$$

где Пр.оз. - продолжительность одного оборота запасов;

П – период в днях;

Поз - оборачиваемость запасов.

Данный показатель позволяет оценить скорость превращения запасов в готовую продукцию и их дальнейшей реализации.

Основными характеристиками потребления материальных ресурсов являются общий и удельный расходы. Общий расход материальных ресурсов представляет собой объем потребления материальных ресурсов, необходимый для выполнения производственной программы в отчетном периоде. В натуральном выражении учитывается общий расход отдельных

видов материальных ресурсов, а суммарный расход различных видов материальных ресурсов выражается в стоимостных показателях [4, с. 59].

Удельный расход (m) определенного типа ресурсов характеризует средний объем его использования на единицу выпущенной продукции. Он вычисляется путем деления общего объема материальных ресурсов, израсходованных на производство данной продукции в отчетном периоде (МР), на объем произведенной годной продукции (Q) (3):

$$m = \frac{МР}{Q} \quad (3)$$

где m - удельный расход материальных ресурсов на единицу продукции;

МР - общий объем израсходованных материальных ресурсов в отчетном периоде;

Q - объем произведенной годной продукции.

Для характеристики эффективности использования материальных ресурсов применяется система обобщающих и частных показателей. К обобщающим показателям относятся материалоёмкость; материалоотдача; коэффициент соотношения темпов роста объёма производства и материальных затрат; удельный вес материальных затрат в себестоимости продукции; коэффициент использования материалов.

Материалоемкость товарной продукции является обобщающим стоимостным показателем, который отражает объем материальных затрат на единицу стоимости товарной продукции предприятия, объединения, подотрасли или отрасли. Показатель рассчитывается по формуле (4):

$$МЕ = \frac{МЗ}{ВП} \quad (4)$$

где МЕ - материалоёмкость продукции;

МЗ - материальные затраты на производство продукции;

ВП - стоимость произведенной продукции.

Материалоотдача определяется как отношение стоимости продукции к общей сумме затрат на материальные ресурсы. Показатель демонстрирует, сколько единиц продукции получено с использованием единицы стоимости материальных ресурсов (сырье, материалы, топливо, энергия и т.д.). Формула расчета показателя выглядит следующим образом (5):

$$МО = \frac{ВП}{МЗ} \quad (5)$$

где МО – материалоотдача;

СП - стоимость произведенной продукции;

МЗ - общая стоимость затрат на материальные ресурсы.

Коэффициент соотношения темпов роста производства и материальных затрат определяется отношением индекса выручки к индексу затрат на материальные ресурсы [5, с. 406] и отражает динамику материалоотдачи, а также раскрывает факторы ее изменения.

Доля материальных затрат в общей стоимости продукции рассчитывается как отношение суммы затрат на материальные ресурсы к общей себестоимости продукции. Изменение показателя отражает динамику материалоемкости продукции [5, с. 407].

Среди совокупных показателей также стоит выделить прибыль на единицу затрат на материальные ресурсы – это наиболее обобщающий показатель эффективности использования материальных ресурсов. Он рассчитывается как отношение суммы прибыли от основной деятельности к общим затратам на материальные ресурсы [6, с. 12]. Увеличение показателя характеризует положительные тенденции в осуществлении хозяйственной деятельности предприятия.

Таким образом, рассмотренные показатели важны для определения потенциала повышения эффективности использования материальных ресурсов предприятия, идентификации областей для возможной экономии ресурсов и оптимизации затрат на материальные ресурсы, что в свою очередь ведет к повышению прибыли предприятия.

Учитывая все вышеизложенное, можно сделать следующие выводы.

1. Необходимым условием организации производства является обеспечение его материальными ресурсами: сырьем, материалами, топливом, энергией, полуфабрикатами и т.д. В рамках производственного цикла материальные ресурсы подвергаются трансформации в материальные затраты, что подчеркивает значимость экономически рационального их использования с целью минимизации себестоимости продукции.

2. Эффективное использование запасов материальных ресурсов позволяет добиться увеличения уровня эффективности использования всех ресурсов, а также повысить скорость обращения вложенного капитала. Для достижения большей операционной эффективности необходимо применять эффективные модели управления запасами, которые могут помочь предприятию увеличить оборот и максимизировать его прибыль. В связи с этим рекомендуется реализация соответствующих механизмов контроля и мониторинга с целью минимизации потерь и оптимизации использования материальных ресурсов.

Библиографический список

1. Экономика предприятия : Учебник для вузов / С. П. Кирильчук, Е. В. Наливайченко, Н. М. Ветрова [и др.]. – Москва : Общество с ограниченной ответственностью «Издательство ЮРАЙТ», 2022. – 417 с. – (Высшее образование)
2. Шульгина, Л. М. Бизнес-планирование развития предприятия / Л. М. Шульгина, А. Н. Нечай // Международный научный журнал Интернаука. – 2018. – Т. 2, № 9(49). – С. 53-57.

3. Медведева, А. Д. Методология управления запасами на предприятии / А. Д. Медведева // Человек. Социум. Общество. – 2022. – № 12. – С. 153-155.
4. Жигарева, Е. Л. Система показателей эффективности использования материальных ресурсов предприятия и новый подход к прогнозированию их уровня / Е. Л. Жигарева, Л. А. Кононова // Вектор экономики. – 2021. – № 11. – С. 54-60.
5. Сулейманова, Д. А. Анализ использования материальных ресурсов / Д. А. Сулейманова, З. Д. Джалилова // Экономика и социум. – 2020. – № 2(69). – С. 405-407.
6. Кнурова, К. А. Материально-производственные запасы как значимый объект учета и анализа / К. А. Кнурова // Проблемы научной мысли. – 2017. – Т. 6, № 1. – С. 10-14.

УДК 338.43.02

Головина С. Г..

д.э.н., профессор, главный научный сотрудник
ФГБОУ ВО «Уральский государственный аграрный университет»
Россия, Екатеринбург

Golovina S. G., Doctor of Economics, Professor
Chief Researcher
Federal State Budgetary Educational Institution of Higher Education "Ural State Agrarian University"
Russia, Yekaterinburg

Развитие сельских кооперативов в Гане: теоретические основания и практические тенденции

Rural cooperative development in Ghana: theoretical foundations and practical trends

Аннотация. В республике Гана, как и в большинстве других африканских стран, имеется большое количество организаций, преследующих не только экономические, но и социальные, и экологические цели. Как правило, такие организации, с одной стороны, придерживаются сформулированным местными сообществами целям, с другой стороны, принадлежат и контролируются лицами, пользующимися их услугами. Тем не менее, трудно дать надёжную оценку масштабам и важности социальной экономики Ганы, поскольку многие из этих организаций, принадлежащих пользователям, являются неформальными организациями (большинство из них не признаны юридически и не зарегистрированы согласно действующему законодательству). Аналитическая информация и официальные данные об этих организациях также, как правило, появляется лишь эпизодически и носит разрозненный характер. На основании результатов имеющихся научных исследований и отчётных материалов в данной статье, в связи с этим, представлены некоторые обобщения относительно состояния и перспектив развития сельских кооперативов в границах сельских территорий Республики Гана. Основной научный вывод сводится к тому, что африканские кооперативы, исходя из теории жизненного цикла кооперативных структур, проходят обычные фазы такого цикла и имеют перспективы на успешное развитие в том случае, если своевременно адаптируются к происходящим во внешней среде переменам. Существенное значение для развития кооперации в стране имеет кооперативное образование, а также государственная поддержка местных инициатив и кооперативных проектов.
Ключевые слова: Республика Гана, социальная экономика, местные ресурсы, социальные предприятия.
Annotation. In the Republic of Ghana, as in most other African countries, there are a large number of organizations pursuing not only economic, but also social and environmental goals. Typically, such organizations, on the one hand, adhere to the goals formulated by local communities, on the other hand, are owned and controlled by the people using their services. However, it is difficult to reliably assess the size and importance of Ghana's social economy because many of these user-owned organizations are informal organizations (most of them are not legally recognized or registered under current legislation). Analytical information and official data about these organizations also, as a rule, appear only sporadically and are fragmented. Based on the results of available scientific research and reporting materials, this article, in this regard, presents some generalizations regarding the state and prospects for the development of rural cooperatives within the boundaries

of rural areas of the Republic of Ghana. The main scientific conclusion is that African cooperatives, based on the theory of the life cycle of cooperative structures, go through the usual phases of such a cycle and have prospects for successful development if they promptly adapt to changes occurring in the external environment. Cooperative education, as well as state support for local initiatives and cooperative projects, are essential for the development of cooperation in the country.
Key words: Republic of Ghana, social economy, local resources, social enterprises.

Как демонстрируют результаты опубликованных в научных журналах исследований, основными формами предприятий социальной экономики в Республике Гана являются сельскохозяйственные кооперативы и объединения производителей, охватывающие различные сферы сельской экономики [1]. Появление таких предприятий в Гане было вызвано, в большей степени, необходимостью противостоять растущей бедности сельского населения и усилить позиции мелких фермеров на национальном и международном рынках, одновременно избегая возврата к централизованной и неэффективной кооперативной модели прошлого. Эволюция развития организаций социальной экономики такова, что по мере того, как сельскохозяйственные кооперативы выходили из-под контроля фермеров в государственные и элитарные фирмы, добровольные объединения производителей становились более предпочтительными формами взаимодействия фермерских домохозяйств [2]. Этому организационному переходу способствовало решение правительства Ганы начать пересмотр действующего закона о кооперативах (Декрета о кооперативных обществах от 1968 года) с целью формального признания объединений производителей в качестве автономных субъектов агробизнеса. В дополнение к этому, появлению и развитию новых объединений способствовало значительное количество внешних стимулов. К примеру, поскольку объединения производителей способствовали снижению операционных издержек и рисков, с которыми сталкиваются программы развития, организованные в поддержку мелких сельских землевладельцев, участие в объединениях вскоре становится важным предварительным условием для участия фермеров в соответствующих программах [1].

Исторические данные, представленные в научной литературе и обзорных материалах аналитиков, подтверждают, что сегодня объединения производителей в сельской Гане являются, по сути, сельскими кооперативами, принадлежащими пользователям. Опираясь на теорию «кооперативного жизненного цикла», предложенную американскими учёными во главе с М. Куком, можно утверждать, что современные кооперативы Ганы развиваются в соответствии с изложенным в данной

теории алгоритмом [3]. В упрощённом виде эта теория объясняет их возникновение при наличии строгого экономического обоснования, которое способствует росту членства до тех пор, пока не начнут возникать проблемы, ведущие либо к краху, либо к переосмыслению организации. На первом этапе фиксируется рост числа членов, подкрепленный перспективой использования преимуществ экономии за счёт размеров и масштаба деятельности. Далее, по мере своего роста, кооперативы имеют тенденцию выходить за пределы своих первоначальных границ, способствуя неоднородности социально-экономических предпочтений участников. Учитывая, что кооперативы обычно создаются на основе классических кооперативных принципов и особой структуры прав собственности, их эволюция приводит к растущей неоднородности в предпочтениях членов и к усложнению модели функционирования, что способствует максимальному распределению рисков между участниками [4]. Однако, в то же время, трансформация внутреннего устройства приводит к возникновению проблемы «безбилетника», возникающей в том случае, если некоторые члены получают выгоду от инвестиций, сделанных организацией, но не являющейся заслугой данных лиц [5]. Рост проблемы безбилетников приводит к коллективному уклонению от активного участия в кооперативной деятельности и, таким образом, к ослаблению конкурентных позиций кооператива и его членов.

Важно подчеркнуть, что и другие «болезни» современных кооперативов, в большей степени присущие европейским и американским кооперативам, наблюдаются у некоторых (наиболее крупных) сельских кооперативов Ганы. Как отмечает Й. Нилссон, проблемы, с которыми сталкиваются сельскохозяйственные кооперативы в странах Африки, не всегда могут быть связаны с неоднородностью рисковых предпочтений членов [4]. Дело в том, что рост числа членов приводит к уменьшению социального капитала, так как социальный капитал действительно имеет тенденцию сокращаться по мере того, как членство становится больше, а сами члены становятся в определённой мере трудно идентифицируемыми. Низкий уровень социального капитала побуждает организации, характеризующиеся слабо специфицированными правами собственности, вкладывать всё больше ресурсов в мониторинг деятельности своих членов и в обеспечение соблюдения имеющихся в обществе требований (в том числе формальных) [6]. Однако, по мере увеличения затрат на мониторинг и правоприменение, доходы имеют тенденцию к снижению и всё больше захватываются сельской элитой. Это означает, что и в среде африканской кооперации встречается проблема агентских издержек, вероятность возникновения которой обратно пропорциональна вероятности возникновения проблемы безбилетника [7]. В контексте Африки проблемы с агентскими издержками обычно способствуют дополнительным продажам

продукции членами кооперативы не коллективно, а индивидуально, по маркетинговым каналам, отличным от кооперативных, а также постепенному оттоку членов из организации в ущерб развитию социальной экономики. Следовательно, рост объединений производителей (и конкретно кооперативов) неизбежно ограничивается ростом либо агентских издержек, либо проблемой «безбилетника». Признание этих проблем мотивирует кооперативы, в одной ситуации, к трансформации организационного устройства кооператива, в другой ситуации – к укреплению традиционных кооперативных принципов.

Анализ имеющихся данных показывает, что подавляющее большинство (89 %) ганских кооперативов, согласно структуре жизненного цикла, находится либо на первой, либо на третьей фазе своего развития, и лишь оставшиеся 11 % демонстрируют динамичное развитие и стабильность. Другими словами, многие кооперативы в Гане находятся в процессе становления их коллективной деятельности, в то время как некоторые из них сталкиваются с проблемами крупных коллективных структур, ведущими их к высоким рискам и неопределённости [8]. Ещё один важный вывод, следующий из результатов анализа структуры ганских кооперативов, заключается в том, что пока данные сельские организации не могут играть той роли, которая позволила бы фермерам всецело распределять риски, повышать эффективность деятельности, выигрывать конкуренцию с крупными сельскохозяйственными производителями. Тем не менее, анализ также демонстрирует, что социально-экономические условия ганских фермеров могут существенно улучшиться, если численность устойчивых кооперативов будет расти, а их потенциал повышаться за счёт новых членов и государственной поддержки. Хотя многие программы развития кооперации в Гане оцениваются как довольно успешные и служат содействию создания кооперативных структур посредством предоставления различных стимулов, государство в настоящее время прилагает дополнительные усилия, чтобы помочь им лучше управлять ростом членства, предотвращать несоответствие между неоднородностью в предпочтениях членов в отношении риска и оптимальностью коллективных инвестиций.

В заключение отметим, что для становления рассматриваемого феномена в Гане существенное значение имеет система кооперативного образования. Как многие европейские, американские и другие кооперативные сообщества делают в подготовке лидеров акцент на высококачественное образование (к примеру, в Университете Миссури есть специальные программы для обучения менеджеров сельскохозяйственных кооперативов, известные своим качеством во всём мире), так и молодёжь в Гане, планирующая свою вовлечённость в кооперативную деятельность, считает обязательным участвовать в аналогичных программах по мере возможности. Более того, реализуемая в стране программа обучения кооперации

выстраивается на активном взаимодействии между кооперативными менеджерами и исследователями, способствуя одновременному развитию теоретических знаний и практических навыков. В итоге, её реализация в Республике Гана способствует и дальнейшим исследованиям в данном направлении, и формированию необходимых компетенций по управлению кооперативами и другими организациями социальной экономики.

Библиографический список:

1. Salifu A., Francesconi, G. N., Kolavalli S. A Review of Collective Action in Rural Ghana, Discussion Paper 00998, Washington, DC: International Food Policy Research Institute, 2010.
2. Smyth R. The roots of Community Development in Colonial Office Policy and Practice in Africa // Social Policy & Administration. 2004. № 38 (4). P. 418-436.
3. Cook M. L. A Life Cycle Explanation of Cooperative Longevity // Sustainability. 2018. №10 (5). P. 1586-1606.
4. Nilsson J. Agricultural Cooperative Development and Institutional Change: Swedish examples from 1990 to 2020 // Journal on Food System Dynamics. 2022. No. 13 (2). P. 115-127.
5. Grashuis J., Cook M. L. An Examination of New Generation Cooperatives in the Upper Midwest: Successes, Failures, and Limitations // Annals of Public and Cooperative Economics. 2018. Vol. 89(4). P. 623-644.
6. Caire G., Tadjudje W. Toward a Global Legal Culture of the SSE Enterprise? An International Comparison of SSE Legislation // RECMA. 2019. №. 353. P. 74-88.
7. Golovina S., Mikolaychik I., Poltarykhin A., Zhuravlev P. The Impact of Human Capital on the Success of an Agricultural Cooperative (example of «Arla Foods») // Siberian Journal of Life Sciences and Agriculture. 2021. Vol.13. № 2. P. 262-283.
8. Grashuis J, Cook M. L. Members of Cooperatives: More Heterogeneous, Less Satisfied? // International Food and Agribusiness Management Association. 2021. No.24 (5). P. 813-825.

Химические науки

DOI 10.34755/IROK.2024.36.86.026

УДК 544.52

Дягилева Елена Павловна,
кандидат химических наук,
доцент кафедры фармацевтической и общей химии

ФГБОУ ВО Кемеровский государственный медицинский университет Минздрава России
Россия, г. Кемерово

Dyagileva Elena Pavlovna,
PhD in Chemistry,
Associate Professor of the Department of Pharmaceutical and General Chemistry
Federal State Budgetary Educational Institution of Higher Education
Kemerovo State Medical University of the Ministry of Health of Russia
Russia, Kemerovo

Идентификация полос в ИК спектрах диффузного отражения нитратов щелочноземельных металлов, облученных светом длиной волны 253,7 нм

Identification of bands in the IR diffuse reflection spectra of alkaline earth metal nitrates irradiated with light with a wavelength of 253.7 nm

Аннотация. Получены ИК спектры диффузного отражения необлученных и облученных светом длиной волны 253,7 нм поликристаллических нитратов щелочноземельных металлов. Максимумы в спектрах диффузного отражения в необлученных нитратах содержат линии разной интенсивности. Волновые числа колебаний нитрат иона в поликристаллических щелочноземельных нитратах следующие: ν_1 ~ 1050 см$^{-1}$; ν_2 (A_2'') ~ 818 см$^{-1}$; ν_3 (E') и ν_4 (E') ~ 1350-1440 см$^{-1}$ и 700-750 см$^{-1}$, соответственно. В колебательных спектрах образцов кристаллогидратов нитратов кальция и магния наблюдаются характерные полосы воды в области 3200-3550 см$^{-1}$ и 1630-1700 см$^{-1}$. На основании полученных инфракрасных спектров диффузного отражения поликристаллических нитратов щелочноземельных металлов, облученных светом длиной волны 253,7 нм установлено, что фотоиндуцированные полосы при 1238-1252 и 822-825 см$^{-1}$ обусловлены нитрит ионами, а полосы при ~ 840, 846, 946, 960 и 1487 см$^{-1}$ отнесены к колебаниям пероксонитрит иона.

Ключевые слова: нитраты щелочноземельных металлов, ИК спектры диффузного отражения, нитрат ион, нитрит ион, пероксонитрит ион.

Annotation. IR diffuse reflection spectra of polycrystalline nitrates of alkaline earth metals, unradiated and irradiated by light with a wavelength of 253.7 nm, were obtained. The maxima in the diffuse reflection spectra in nonradiated nitrates contain lines of different intensities. The wave number of the fluctuations in the nitrate ion in polycrystalline alkaline earth nitrates following: ν_1 ~ 1050 cm^{-1}; ν_2 (A_2'') ~ 818 cm^{-1}; ν_3 (E') and ν_4 (E') ~ 1350-1440 cm^{-1} and 700-750 cm^{-1}, respectively. In the vibrational spectra of samples of calcium and magnesium

nitrate crystallohydrates, characteristic bands of water are observed in the range of 3200-3550 cm^{-1} and 1630-1700 cm^{-1}. Based on the obtained infrared diffuse reflection spectra of polycrystalline nitrates of alkaline earth metals irradiated with light with a wavelength of 253.7 nm, it was found that the photoinduced bands at 1238-1252 and 822-825 cm^{-1} are due to nitrite ions, and the bands at ~ 840, 846, 946, 960 and 1487 cm^{-1} are attributed to fluctuations of the peroxonitrite ion.
Key words: alkaline earth metal nitrates, IR diffuse reflection spectra, nitrate ion, nitrite ion, peroxonitrite ion.

Нитраты щелочных и щелочноземельных металлов во многих исследованиях используют для изучения процессов распада\разложения, протекающих в твердой фазе или в растворе при взаимодействии ионизирующего излучения с веществом. Предложены разные механизмы фотолиза нитратов [1-6], однако все они имеют разногласия, включающие несовпадение результатов, полученных в твердой фазе и в растворе. Тем не менее однозначно установлено, что в результате фотолиза нитратов основными продуктами являются нитрит и пероксонитрит ионы и кислород [1-6].

В современном мире интерес к химии пероксонитрит иона и пероксоазотистой кислоты очень огромен, что связано с его обнаружением *in vivo*, подтверждением его важной роли в физиологических процессах, химии атмосферы и природных вод [7-10].

Изучение химических реакций пероксоазотистой кислоты и пероксонитрит иона связано с рядом проблем, обусловленных их высокой химической активностью пероксонитрит иона и кислоты, а также с разнообразием способов разложения и изомеризации пероксонитрит иона как в растворе, так и в твердой фазе, влиянием на скорость реакций и механизмы диссоциации или изомеризации пероксоазотистой кислоты и пероксонитрит иона многих факторов [11-27]: кислотности среды, температуры, ионов тяжелых металлов, оксида углерода (IV), присутствие органических соединений, структуры (*цис*- и *транс*-изомеры) пероксонитрит иона и его концентрации, наличия воздействия ионизирующего излучения разной энергии и интенсивности.

В связи с существующими проблемами для более корректного моделирования механизмов разложения и изомеризации пероксонитрит иона в твердой фазе в настоящей работе были изучены ИК спектры диффузного отражения необлученных и облученных УФ светом с длиной волны 253,7 нм поликристаллических нитратов щелочноземельных металлов и проведена идентификация полос колебательных спектров, на основе имеющихся литературных данных.

Экспериментальная часть

Измерение ИК спектров диффузного отражения

Для регистрации ИК спектров использовали спектрометр инфракрасного диапазона с фурье-преобразованием Tenzor 27 фирмы Bruker с приставкой диффузного отражения EasyDiff фирмы PIKE Tech, с применением пакета программ OPUS 50 и программы калибровки по стандартным образцам. Стандартные образцы – пары воды; пленки из полистирола; стеклянный фильтр – прилагаются к прибору.

Подготовка образцов нитратов щелочноземельных металлов

Трижды перекристаллизованные соли нитратов щелочноземельных металлов размалывали в агатовой шаровой мельнице, отсеивали фракцию не более 0,1 мм. После чего перемешивали с бромидом калия в соотношении 1:10 $M(NO_3)_2$:KBr, где M = Ba, Sr, Ca и Mg. Затем производили запись спектров необлученных нитратов и облученных нитратов. Облучали образцы светом с длиной волны 253,7 нм заданное время, используя лампы ДБ-30, интенсивность потока излучения на длине волны 253,7 нм равна $(1,6\pm0,1)\cdot10^{15}$ квант·см$^{-2}$·с$^{-1}$).

Измерение спектров проводили с разрешением 4 см$^{-1}$ и областью измерений 400 – 4000 см$^{-1}$. В качестве стандарта использовали KBr.

Спектры диффузного отражения преобразованы посредством функции Кубелка-Мунка. Эта функция применялась при аналитическом разделении контуров сложных полос спектров диффузного отражения.

Все экспериментальные данные получены при 22°С.

Результаты и обсуждение

ИК спектры необлученных щелочноземельных нитратов

В работе [28] показано, что «свободный» нитрат-ион должен быть плоским, и относится к точечной группе D_{3h}. Ион нитрата обладает шестью нормальными колебаниями, которые вырождаются до четырех при наличии у иона оси симметрии третьего порядка (D_{3h}). Симметричное валентное колебание $\nu_1(A_1')$, согласно правилам отбора, не должно наблюдаться в ИК спектре плоского иона нитрата симметрии D_{3h}, но становится разрешенным при любой другой геометрии NO_3^-. В действительности, нитрат ион в различных кристаллах нитратов металлов имеет симметрию C_1, C_S, C_{2V}, C_{3V} и D_{3h}. Колебание ν_1 наблюдается в области ~ 1050 см$^{-1}$. Внеплоскостное колебание ν_2 (A_2'') активно в ИК спектре и проявляется обычно при ~ 830-840 см$^{-1}$. Антисимметричные валентные колебания ν_3 (E') и ν_4 (E') активны в ИК спектре и наблюдаются при 1350-1390 см$^{-1}$ и 700-730 см$^{-1}$, соответственно. Колебания ν_3 и ν_4 и их обертоны являются вырожденными.

Таблица 1

Волновые числа колебаний нитрат иона в образцах состава $M(NO_3)_2$:KBr (1:10)

Матрица	Волновое число, см$^{-1}$

	ν_1	ν_2	ν_3	ν_4	$2\nu_4$
$Ba(NO_3)_2$	1047	819	1356, 1415	731	1462
	1047	818	1370, 1418	730	–
$Sr(NO_3)_2$	1056	816	1438, 1379	737	1474
	1056	816	1440, 1382	738	–
$Ca(NO_3)_2 \cdot 4H_2O$	1050	817	1442, 1389	750	1456
	1050	818	1434, 1382	750	1457
$Mg(NO_3)_2 \cdot 6H_2O$	1059	816	1396	–	–
	1059	819	1389	727	1457

Колебательные спектры исследуемых образцов щелочноземельных нитратов содержат линии разной интенсивности, максимумы которых приведены в таблице 1. На рис. 1 приведен спектр необлученного образца $Ca(NO_3)_2$ H_2O. Полученные результаты показывают хорошее совпадение с литературными данными [29-32].

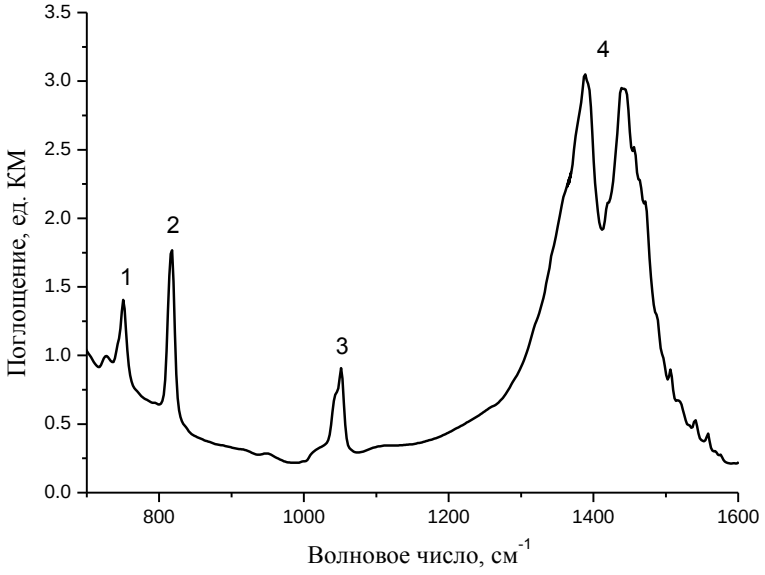


Рис. 1. ИК спектр диффузного отражения образца $Ca(NO_3)_2 \cdot H_2O$:KBr:
1 - колебание ν_4, 2 - колебание ν_2, 3 – колебание ν_1, 4 – колебание ν_3

В колебательных спектрах образцов кристаллогидратов нитратов кальция и магния наблюдаются характерные полосы воды в области 3200-3550 $см^{-1}$ (антисимметричные и симметричные валентные колебания OH) и 1630-1700 $см^{-1}$ (деформационные колебания HOH) [32].

Линии, отнесенные к полносимметричному колебанию иона нитрата ν_1 в $Ba(NO_3)_2$, $Sr(NO_3)_2$ и $Mg(NO_3)_2 \cdot 6H_2O$ имеют небольшую интенсивность, что может свидетельствовать о незначительном отклонении симметрии аниона от D_{3h}. Для $Ca(NO_3)_2 \cdot 4H_2O$ возможно это отклонение достаточно велико, поэтому наблюдаются интенсивные линии.

ИК спектры щелочноземельных нитратов, облученных светом длиной волны 253,7 нм

При облучении образцов состава $M(NO_3)_2$:KBr (1:10) наблюдаются изменения в колебательных спектрах. Как видно на рис. 2 в спектре $Ca(NO_3)_2 \cdot 4H_2O$:KBr появляется дополнительный набор линий, обусловленных нитрит и пероксонитрит ионами (таблица 2). Интенсивность линий зависит от времени экспозиции.

Идентификация полос, обусловленных нитрит и пероксонитрит ионами, проводилась на основе имеющихся литературных данных [33-36]. В работе [33] показано, что ИК спектр кристаллов нитрата бария, сокристаллизованных с ионами NO_2^- имеет три основных колебания ионов нитрита: $\nu_1 = 1325$ см$^{-1}$ $\nu_2 = 825$ см$^{-1}$, $\nu_3 = 1255$ см$^{-1}$.

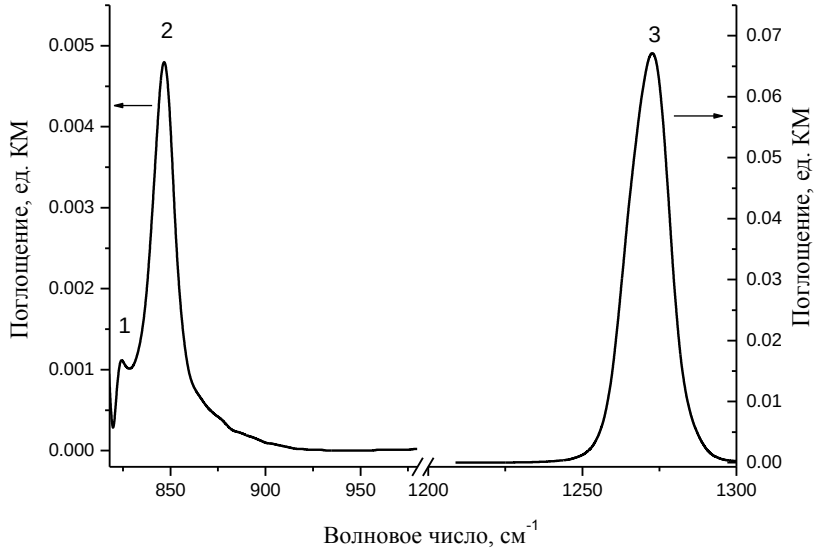


Рис. 2. ИК спектр диффузного отражения образца $Ca(NO_3)_2 \cdot 4H_2O$:KBr после фотолиза 120 мин светом λ=253,7 нм. 1,3 – NO_2^-, 2 – $ONOO^-$

Таблица 2

Волновые числа колебаний ионов в образцах состава $M(NO_3)_2$:KBr (1:10) после облучения λ 253,7 нм

Матрица	Волновое число, см$^{-1}$					
	NO_2^-		$ONOO^-$			
$Ba(NO_3)_2$	1250	825	960	946	840	–
$Sr(NO_3)_2$	1253	822	–	946	–	–
$Ca(NO_3)_2 \cdot 4H_2O$	1238	828	960	–	846	–
$Mg(NO_3)_2 \cdot 6H_2O$	1252	825	960	–	–	1487

Полосы при 1238-1252 и 822-825 $см^{-1}$ идентифицированы как колебания, обусловленные нитрит ионами, а полосы при ~ 840, 846, 946, 960 и 1487 $см^{-1}$ отнесены к колебаниям пероксонитрит иона.

При фотолизе образцов щелочноземельных нитратов светом 253,7 нм наблюдается увеличение интенсивности полносимметричного колебания в области 1047-1059 $см^{-1}$, которое мы связываем с ростом разупорядоченности кристаллической решетки, приводящей к искажению ионов нитрата.

Таким образом, измерение инфракрасных спектров диффузного отражения облученных щелочноземельных нитратов позволило подтвердить образование пероксонитрит и нитрит ионов в качестве продуктов разложения. Других продуктов фотолиза не обнаружено.

Заключение

На основании полученных инфракрасных спектров диффузного отражения поликристаллических порошков нитратов щелочноземельных металлов, необлученных и облученных светом длиной волны 253,7 нм и последующего сравнения с литературными данными, позволяет нам сделать вывод о том, что фотоиндуцированные полосы при 1238-1252 и 822-825 $см^{-1}$ идентифицированы как колебания, обусловленные нитрит ионами, а полосы при ~ 840, 846, 946, 960 и 1487 $см^{-1}$ отнесены к колебаниям пероксонитрит иона.

Библиографический список:

1. Plumb R. C., Edwards J. O. Color Centers in UV–Irradiated Nitrates // J. Phys. Chem. 1992. V.96. №8. P. 3245–3247.

2. Юрмазова Т. А. Роль пернитрита в превращениях иона нитрата под действием излучений: автореф. дис. …канд. хим. наук / Т.А. Юрмазова; ЛТИ, – Ленинград, 1989.

3. Невоструев В. А. Роль низкоэнергетических возбужденных состояний иона нитрата в фотолизе и радиолизе кристаллов нитратов щелочных металлов // Хим. высок. энерг. 1986. Т.20. №5. С.425–429.

4. Невоструев В. А., Миклин М. Б. Фотолиз и радиолиз кристаллических нитратов щелочных металлов // Хим. высок. энерг. 1987. Т.21. №2. С. 154–158.

5. Миклин М. Б., Ананьев В. А., Лырщиков С. Ю., Нелюбина Н. В., Скибина А. В. Образование пероксонитрита и нитрита при фотолизе кристаллических нитратов // Ползуновский вестник. 2006. № 2–1. С. 53–56.

6. Сериков Л. В., Юрмазова Т. А., Шиян Л. И. Образование пернитрит и нитрит-ионов в нитратах щелочных металлов // Томский политехнический институт. Томск. 1987. С. 195 – 201. Деп. в ОНИИТЭХИМ, №1075–хп–86.

7. Лобачев В. Л., Рудаков Е. С. Химия пероксинитрита. Кинетика и механизмы реакций // Ж. Успехи химии. 2006. V. 75. №5. С. 422–444.

8. Bock J., Jacobi H.-W. Development of a Mechanism for Nitrate Photochemistry in Snow // J. Phys. Chem. A. 2010. V. 114. № 4. P.1790–1796

9. Yabushita A., Iida D., Hama T., Kawasaki M. Direct Observation of OH Radicals Ejected from Water Ice Surface in the Photoirradiation of Nitrate Adsorbed on Ice at 100 K // J. Phys. Chem. A. 2008. V. 112. № 40. P. 9763–9766.

10. Koppenol W. H. The chemistry of peroxynitrite, a biological toxin // Química nova. 1998. V. 21. № 3. P. 326–331.

11. Squadrito G. L., Pryor W. A. Oxidative Chemistry of Nitric Oxide: The Roles of Superoxide, Peroxynitrite, and Carbon Dioxide // Free Radical Biology & Medi-cine. 1998. V. 25. № 4/5. P. 392–403.

12. Lymar S. V., Hurst J. K. Rapid Reaction between Peroxonitrite Ion Carbon Dioxide: Implication of Biological Activity // J. Am. Chem. Soc. 1995. V.117. № 34. P. 8867–8868.

13. Kissner R., Koppenol W. H. Product Distribution of Peroxynitrite Decay as a Function of pH, Temperature, and Concentration // J. Am. Chem. Soc. 2002. V.124. №2. P. 234 239.

14. Plumb R. C., Edwards J. O. Problem of Concurrent Measurements of Peroxonitrite and Nitrite Contents // Analyst. 1992. V. 117. P. 1639-1641.

15. Дягилева Е. П. Изомеризация и диссоциация пероксонитрит иона при растворении кристаллического нитрата калия, облученного светом длиной волны 253,7 нм // VI Российская конференция (с приглашением специалистов стран СНГ) «Актуальные проблемы химии высокий энергий»: сборник статей. Москва, 2015. С. 170 175.

16. Дягилева Е. П., Миклин М. Б. Изомеризация и диссоциация пероксонитрит иона при растворении кристаллического нитрата калия, облученного светом длиной волны 253,7 нм // Вестник Кемеровского государственного университета. 2015. №4-3 (64). С. 233 236.

17. Дягилева Е. П., Миклин М. Б., Ананьев В. А. Вторичные темновые процессы в нитратах щелочноземельных металлов, облученных светом 253,7 нм // Ползуновский вестник. 2014. №3. С. 58 61.

18. Кригер Л. Д., Миклин М. Б., Дягилева Е. П., Ананьев В. А. Изомеризация и диссоциация пероксонитрит иона при растворении кристаллического нитрата калия, облученного светом длиной волны 253,7 нм // Журнал физической химии. 2013. Т.87. №2. С. 326.

19. Дягилева Е. П. Фотолиз нитратов щелочноземельных металлов: дис. … канд. хим. наук / Кемеровский государственный университет: Кемерово, 2011. – 137 с.

20. Дягилева Е. П., Миклин М. Б., Нелюбина Н. В. Образование транс-пероксонитрита при фотолизе кристаллических нитратов // Известия вузов. Физика. 2011. Т.54. №1-2. С. 244 247.

21. Pak V. K., Anan'Ev V. A., Miklin M. B., Rezvova M. A., Dyagileva E. P., Lyrshchikov S. Y. Conformer of the peroxynitrite ion formed under photolysis of crystalline alkali nitrites – cis or trans? // IOP Conference Series: Materials science and Engineering. 2017. С. 012091.

22. Дягилева Е. П., Миклин М. Б., Нелюбина Н. В. Образование транс-пероксонитрита при фотолизе кристаллических нитратов // Радиационно-термические эффект и процессы в неорганических материалах: сб. трудов VII международной научной конференции. Кемерово, 2010. С. 521 524.
23. Tsai J.H.M., Harrison J.G., Martin J.C., Hamilton T.P., M. van der Voerd, Jablonsky M.J., Beckman J.S. Role of Conformation of Peroxynitrite Anion ($ONOO^-$) with Its Stability and Toxicity // J.Am.Chem.Soc. 1994. V.116. №9. P. 4115–4116.
24. Koppenol W.H. The basic chemistry of nitrogen monoxide and peroxynitrite // Free Radic.Biol.Med. 1998. V.25. №4/5. P. 385–391.
25. Дягилева Е. П., Миклин М. Б., Нелюбина Н. В., Шрайбман Г. Н. Фотолиз нитратов металлов второй группы // Известия вузов. Физика. 2008. Т.51. №11-3. С. 195 198.
26. Дягилева Е. П., Миклин М. Б., Нелюбина Н. В., Шрайбман Г. Н. Фотолиз нитратов щелочноземельных металлов // Фундаментальные проблемы современного материаловедения. 2008. Т.5. №3. С. 7 10.
27. Дягилева Е. П. Идентификация полос в спектрах оптического поглощения и диффузного отражения нитратов щелочноземельных металлов, облученных светом длиной волны 253,7 нм // Актуальные проблемы науки и образования в условиях современных вызовов»: материалы XIX Международной научно-практической конференции. Москва, 2023. С. 328 – 336.
28. Walsh A.D. The Electronic Orbitals, Shapes and Spectra of Polyatomic Molecules. Part V Tetratomic, Non–hydride Molecules, AB_3. // J. Chem. Soc. 1953. P. 2301–2306.
29. Addison C. C., Walker A. Anhydrous Nitrates of the Group II Metals // J. Chem. Soc. 1963. № 2. P. 1220.
30. Brooker M. H., Irish D.E., Boyd G.B. Ionic interaction in crystals: infrared and Raman spectra of powdered $Ca(NO_3)_2$, $Sr(NO_3)_2$, $Ba(NO_3)_2$ and $Pb(NO_3)_2$ // J. Chem. Phys. 1970. V. 53. № 4. P. 1083.
31. Bon A. M, Benoit C., Bernard O. Dynamical properties of crystals of $Sr(NO_3)_2$, $Ba(NO_3)_2$ and $Pb(NO_3)_2$ Infrared spectra and structure // Phys. Stat. Sol. 1976. V. 78(b). P.67–78.
32. Накомото К. ИК спектры и спектры КР неорганических и координационных соединений: Пер. с англ. / К. Накомото. М.: Мир, 1991. – 536 с.
33. Нелюбина Н. В. Фотолиз нитрата бария: дисс…канд. хим. наук / Кемеровский государственный университет: Кемерово, 2006. – 116 с.
34. Bannov S. I., Miklin M. B. Drift study of the products formed by radiolysis and photolysis of alkaline nitrates // Radiation Effect & Defects in Solids. 2002. V.157. № 5. P. 509–514.

35. Liang B., Andrews L. Infrared Spectra of cis- and trans-Peroxynitrite Anion, $OONO^-$, in Solid Argon // J. Am. Chem. Soc. 2001. V. 123. № 40. P.9848–9854.
36. Кригер, Л.Д. Фотолиз нитрат-ионов в матрицах неорганических солей: дисс…канд. хим. наук / Кемеровский государственный университет: Кемерово, 2006. – 137 с.

Юридические науки

УДК 343.9

Кобец Петр Николаевич
д.ю.н., профессор
главный научный сотрудник
Всероссийский научно-исследовательский
институт МВД России (ФГКУ «ВНИИ МВД России»)
Россия, Москва

Kobets Petr Nikolaevich
Doctor of Law,
Professor
Chief Researcher
All-Russian Scientific Research
Institute of the Ministry of Internal Affairs of Russia
(FGKU "VNII MIA of Russia")
Russia Moscow

Характеристика потенциальных субъектов киберугроз и мер, направленных на борьбу с ними

Characteristics of potential subjects of cyber threats and measures aimed at combating them

Аннотация. В проведенном научном исследовании, автором дана характеристика субъектов киберугроз, которая дает представление о том, как преступниками могут быть использованы разнообразные методы для достижения собственных преступных целей в киберпространстве. Категория киберпространство будучи метафорической абстракцией, которую в начале использовали философы сегодня, широко используется в компьютерной сфере, и понимается как виртуальная реальность. Киберпространство в отличии от пространства, является его более расширенной версией, где происходит общение между пользователями телекоммуникационных систем. Повсеместное распространение телекоммуникационных систем, позволяет субъектам киберпреступной деятельности физически находиться в любой точке планеты и влиять на безопасность информационных систем большинства мировых держав. Давая характеристику субъектов киберпреступной деятельности, автором отмечается, что киберпреступниками обладающими наивысшими уровнями мастерства, как правило наносятся самые опасные кибератаки, которые регистрируются в последнее время. Немаловажно и то, что современные киберпреступники стремятся применять ряд наиболее передовых методов по проведению наиболее опасных кибератак. Уже не редкость, когда субъектами киберпреступной деятельности проводятся разного рода разведывательные действия в киберпространстве против целей, которые в перспективе будут подвергаться кибератакам. По имеющимся прогнозным данным расходы на продукты и услуги в области кибербезопасности для защиты от киберпреступности в дальнейшей перспективе будут только увеличиваться. В дальнейшем чрезвычайно важно прогнозировать, в какой именно степени правоохранительная система сможет противостоять киберпреступности, а также при помощи каких мер воздействия на ее вновь возникающие

проявления. Между тем, чтобы активно противодействовать преступной активности в киберпространстве необходимо совершенствовать предупредительные меры, направленные на нейтрализацию киберпреступных проявлений.
Ключевые слова: киберпространство, компьютерная система, киберугрозы, вредоносные программы, субъекты киберугроз, уровень кибербезопасности, правоохранительная деятельность, киберуязвимости, телекоммуникационные системы, вредоносные вирусы, шпионское программное обеспечение, предупреждение преступности.
Annotation. In the scientific research conducted by the author, the characteristics of cyber threat actors are given, which gives an idea of how criminals can use a variety of methods to achieve their own criminal goals in cyberspace. The category of cyberspace, being a metaphorical abstraction that was initially used by philosophers, is now widely used in the computer field and is understood as virtual reality. Cyberspace, unlike space, is its more extended version, where communication takes place between users of telecommunication systems. The widespread distribution of telecommunication systems allows subjects of cybercriminal activity to be physically located anywhere on the planet and influence the security of the information systems of most world powers. Characterizing the subjects of cybercriminal activity, the author notes that cybercriminals with the highest levels of skill usually inflict the most dangerous cyberattacks that have been recorded recently. It is also important that modern cybercriminals strive to use a number of the most advanced methods to carry out the most dangerous cyber attacks. It is no longer uncommon for cybercriminal actors to carry out various types of reconnaissance activities in cyberspace against targets that will be subject to cyber attacks in the future. According to available forecasts, spending on cybersecurity products and services to protect against cybercrime will only increase in the future. In the future, it is extremely important to predict to what extent the law enforcement system will be able to resist cybercrime, as well as with the help of what measures to influence its newly emerging manifestations. Meanwhile, in order to actively counteract criminal activity in cyberspace, it is necessary to improve preventive measures aimed at neutralizing cybercriminal manifestations.

Key words: cyberspace, computer system, cyber threats, malware, cyber threat actors, level of cyber security, law enforcement, cyber vulnerabilities, telecommunication systems, malicious viruses, spyware, crime prevention.

Средой, в которой происходят современные киберугрозы является онлайн киберпространство, в котором субъекты киберугроз осуществляют свои противоправные действия. Сегодня сетями, находящимися в киберпространстве, охватывается вся планета [1, с.161]. Причем среди

пользователей Интернета не только законопослушные граждане, но и лица, занимающиеся противоправной деятельностью, для которых телекоммуникационные сети предлагают множество различных вариантов преступной деятельности, а также укрытий от правоохранителей [2, с.38].

Субъектами киберугроз происходящих в киберпространстве могут быть, как организованные группы, так и отдельные лица, которые умышленно стремятся воспользоваться уязвимостями, низкой осведомленностью о кибербезопасности, или технологическими разработками компьютерных пользователей для получения несанкционированного доступа к информационным системам, с целью противоправного воздействия на данные устройства, системы и телекоммуникационные сети [3, с.232].

Широкое и повсеместное внедрение телекоммуникационных систем, а также глобальное распространение Интернета позволяет субъектам рассматриваемой противоправной деятельности, в большинстве случаев физически находиться в любой точке мира, и влиять на безопасность информационных систем любого государства мира [4, с.112].

Субъектами киберугроз имеющих высший уровень мастерства, как правило наносятся самые опасные кибератаки. Они стараются применять ряд наиболее передовых методов по проведению наиболее опасных кибератак, чтобы достигнуть свои преступные цели [5, с.180].

Начинающие хакеры, как правило, находятся на самом низком уровне сложности по нанесению киберугроз, поскольку они часто полагаются на широко доступные, и распространенные для ведения киберпреступной деятельности инструменты, которые не требуют серьезных технических навыков для проведения кибератак. Их действия, чаще всего, не оказывают серьезного воздействия на защищенные объекты [6, с.30].

Гораздо опаснее инсайдерские угрозы, которые осуществляются благодаря персоналу, работающему в организациях и учреждениях. Подобные субъекты киберпреступной деятельности особенно опасны из-за их доступа к внутренним сетям, великолепно защищенным периметрами безопасности [7, с.161]. Возможность входа в систему является ключевым компонентом для подобных злоумышленников, и наличие привилегированного доступа устраняет необходимость использования других удаленных средств для нанесения кибератаки [8, с.58]. Немаловажно и то, что инсайдерские угрозы могут быть связаны с любым из других типов субъектов угроз. Как правило субъектами подобных киберугроз могут быть недовольные сотрудники подвергшихся инсайдерским кибератакам организаций [9, с.445].

Рядом субъектов киберугроз осуществляются вредоносные действия на основе использования технических уязвимостей отдельных пользователей и организаций, используя методы социальной инженерии, или манипулируя

социальными сетями [10, с.195]. Хорошо технически подготовленные преступники, как правило тщательно выбирает технические устройства и программное обеспечение для осуществления кибератаки. Кибератаки подобных субъектов киберпреступной деятельности, в большинстве случаев и с наибольшей вероятностью приводят к серьезным последствиям [11, с.457].

Иногда такими субъектами проводятся разведывательные мероприятия против цели, которые в последствии будут атакованы. Как правило такими преступниками могут быть использованы разнообразные методы для достижения преступных целей [12, с.179]. Большинство субъектов подобных киберугроз на основе широкомасштабных преступных проявлений используют максимум возможностей для атак в недостаточной степени защищенных телекоммуникационных сетей и при этом похищая цененые базы данных [13, с.347].

Как правило техническими уязвимостями в кибербезопасности эксперты называют в меньшей степени защищенные места, либо имеющие место быть разного рода недостатки в разработке, внедрении, эксплуатации или управлении информационно-технологическими системами, устройствами [14, с.132]. Например, субъектами рассматриваемых угроз могут быть предприняты попытки установки вредоносного программного обеспечения, либо же они могут воспользоваться существующими недостатками в системах кибербезопасности. Однако, помимо установки вредоносного программного обеспечения, субъектами киберугроз также могут быть применены разного рода инструменты, которые непосредственно направлены на конкретные технические уязвимости в кибербезопасности [15, с.110].

В том числе рядом субъектов киберугроз используется социальная инженерия, чтобы обманом заставить пользователей компьютерной техники непреднамеренно разрешить доступ к собственной системе, сети или устройству. Подобные методы киберпреступников, нацеленные на человеческие качества, такие как небрежность и доверие, и в совокупности называются социальной инженерией [16, с.129].

Субъекты киберугроз, также легко могут манипулировать социальными сетями, законными инструментами рекламы, и обмена информацией для проведения онлайн-кампаний, которые могут повлиять на ряд таких событий, как перепись населения или же деятельность кампаний в области общественного здравоохранения, а также на общественный дискурс в более широком смысле [17, с.165].

Обладая весьма неплохим и даже глубоким пониманием того, как работают традиционные средства массовой информации и социальные сети, а также того, как население потребляет информационные данные, участники подробных киберугроз могут продвигать собственные сообщение и

информацию более широким целевым аудиториям с относительно низкими финансовыми и иными затратами [18, с.62]. Кроме того, они также могут все это сделать, маскируясь под законных поставщиков информационных данных, захватывая учетные записи в социальных сетях, или создавая веб-сайты и новые учетные записи [19, с.49].

Шпионское программное обеспечение является вредоносным программным обеспечением, используемым для отслеживания цифровых действий и информации пользователя с ведома или без согласия пользователя. Шпионские программы могут использоваться для многих видов преступной деятельности, включая ведение журнала нажатий клавиш, доступ к микрофону и веб-камере, мониторинг активности пользователей и привычки серфинга, а также захват имен пользователей и паролей [20, с.125].

Вредоносное программное обеспечение обычно доставляется с помощью вирусов, червей и троянов с далеко идущими последствиями. Вирус является исполняемой и воспроизводимой программой, которая вставляет свой собственный код в законные программы с целью повреждения главного компьютера [21, с.150]. В самом простом виде червь является компьютерной программой, предназначенной для самовоспроизведения и распространения на другие компьютеры для истощения ресурсов системы [22, с.117].

Кроме того, как и вирус, червь обладает способностью распространять код, который может повредить программное обеспечение компьютерных систем и вывести их из строя. Такой код называется полезной нагрузкой (например, возможность шифрования файлов в программах-вымогателях и установка системных бэкдоров, обеспечивающих удаленный доступ). Троян-это вредоносная программа, замаскированная под законное программное обеспечение, или встроенная в него, которая имеет цели, сходные с вирусами и червями, но, в отличие от любого из них, не реплицируется и не распространяется самостоятельно [23, с.21].

По оценкам компании Cybersecurity Ventures, в 2022 году киберпреступность обошлась миру в 7 триллионов долларов США. Если бы ее измеряли как страну, то киберпреступность была бы третьей по величине экономикой в мире после США и Китая.

В 2004 году мировой рынок кибербезопасности оценивался в 3,5 миллиарда долларов, а в 2017 году он стоил более 120 миллиардов долларов. Рынок кибербезопасности вырос примерно в 35 раз за этот 13-летний период. По прогнозам, глобальные расходы на продукты и услуги в области кибербезопасности для защиты от киберпреступности в совокупности превысят 1 триллион долларов за пятилетний период с 2017 по 2021 год. Большинство бюджетов кибербезопасности растут линейно или равномерно, но количество кибератак растет экспоненциально. Cybersecurity Ventures прогнозирует ежегодный рост рынка кибербезопасности на 12-15% до 2025

года. Хотя это может быть приличным ростом, он меркнет по сравнению с понесенными затратами от киберпреступности [24, с.45].

Для того чтобы активно противодействовать преступной активности в киберпространстве, помимо обще социального предупреждения рассматриваемых преступных проявлений, в обязательном порядке также необходимы и специальные меры [25, с.448]. Так, например, важна атрибуция кибератак. Так называется акт точного определения субъекта киберугрозы, ответственного за определенный набор действий. Успешная атрибуция субъекта киберугроз важна по многим причинам и в первую очередь, чтобы наиболее активно противостоять киберугрозам. Данный вид деятельности включая сетевую оборону, работу правоохранительных органов, иные методы сдерживание, а также развитие международного сотрудничества с дружественными странами [26, с.115]. Совершенно очевидно, что успешная атрибуция субъекта киберугроз может быть затруднена, поскольку многие субъекты киберпреступной деятельности предпринимают множество усилий, чтобы избежать атрибуции, умело запутывая следы собственной преступной деятельности.

Библиографический список:

1. Обзор II Всероссийской научно-практической конференции «Правовое обеспечение национальной безопасности. Памяти А. А. Прохожева» (РАНХиГС, Москва, 21 апреля 2023 года) / О. Ф. Акбашев, К. В. Алексеев, В. П. Беркут [и др.] // Транспортное право и безопасность. – 2023. – № 4(48). – С. 158-191.

2. Кобец П.Н., Савелов О.П. Методологические проблемы обеспечения общественной безопасности как элемента внутренней безопасности России от угрозы преступности // Предупреждение преступности в системе обеспечения внутренней безопасности: учебное пособие; Московский ин-т права, негос. образовательное учреждение высш. проф. образования. – Москва: Объединенная акад. образовательных учреждений, 2008. – С. 37-63.

3. Пузырева Ю.В., Захарова А.Д. Актуальные направления международного сотрудничества в борьбе с преступлениями, совершаемыми в сфере информационных технологий в отношении детей // Вестник Московского университета МВД России. – 2021. – № 6. – С. 231-234. – DOI 10.24412/2073-0454-2021-6-231-234.

4. Кобец П.Н. Предупреждение преступлений в жилом секторе // Актуальные проблемы гуманитарных наук: Сборник научных трудов / Редколлегия: Галкин В.В. - научный редактор, Ильяшенко А.Н., Фефелов В.М., Юрьева И.Ф. - ответственный секретарь. Том Выпуск 1. – Воронеж: Центрально-Черноземное книжное издательство, 2008. – С. 111-114.

5. Чекунов И.Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. – 2012. – № 3. – С. 178-186.

6. Кобец П.Н. О важности использования комплексных мер по поддержке, продвижению и защите отечественных компетенций в области кибербезопасности // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2023. – № 3. – С. 29-34.

7. Предупреждение преступности в России: Монография / Ю. М. Антонян, М. М. Бабаев, Ю. Г. Касперович [и др.]; Под редакцией профессора Ю. М. Антоняна. – Москва: ОАО «Можайский полиграфический комбинат», 2014. – 344 с.

8. Кобец П.Н. Перспективы совершенствования уголовно-правового регулирования общественных отношений в сфере информационных технологий // Вестник Самарского юридического института. – 2023. – № 1(52). – С. 54-62. – DOI 10.37523/SUI.2023.52.1.008.

9. Машкина И.В., Куприянов А.О. Классификационная схема и модели современных вирусных программ // Информационные технологии. – 2017. – Т. 23, № 6. – С. 443-448.

10. Кобец П.Н. Усиление общесоциального предупреждения преступности посредством профилактики административных правонарушений // Актуальные проблемы гуманитарных наук: Сборник научных трудов / Редколлегия: Галкин В.В. - научный редактор, Ильяшенко А.Н., Кальченко Е.В., Фефелов В.М., Юрьева И.Ф. - ответственный секретарь. Том Выпуск 2. – Воронеж: Воронежский центр научно-технической информации, 2009. – С. 194-197.

11. Попов Е.А., Остапенко Г.А. Dos-атаки на инновационные государственные распределенные информационные системы: риск-анализ при нерегулярном распределении ущерба // Информация и безопасность. – 2014. – Т. 17, № 3. – С. 456-459.

12. Кобец П.Н. О предупреждении рецидива корыстно-насильственных преступлений против собственности // Актуальные проблемы борьбы с преступностью в Сибирском регионе: Сборник материалов научно-практической конференции с международным участием, Красноярск, 14–15 февраля 2008 года / Ответственный редактор: С. Д. Назаров. Том Часть 1. – Красноярск: Сибирский юридический институт МВД России, 2008. – С. 178-180.

13. Кобец П.Н. Концептуально-теоретический подход к определению понятия "экстремизм" // Межнациональное согласие - основа преодоления экстремизма и терроризма, утверждения правового государства: методологический, идеологический, концептуально-теоретический, правовой, аналитико-прогностический аспекты: межведомственный

научный сборник / Комарова А.И. (глав. ред.). Том 4 (42). – Москва: Светлана Зенина, 2012. – С. 346-349.

14. Трубачев Е.С. Троянские программы: механизмы проникновения и заражения // Вестник Волжского университета им. В.Н. Татищева. – 2011. – № 18. – С. 130-134.

15. Кобец П.Н. Предупреждение преступлений, совершаемых в состоянии алкогольного опьянения // Актуальные проблемы гуманитарных наук: Сборник научных трудов / Редколлегия: Галкин В.В. - научный редактор, Ильяшенко А.Н., Фефелов В.М., Юрьева И.Ф. - ответственный секретарь. Том Выпуск 1. – Воронеж: Центрально-Черноземное книжное издательство, 2008. – С. 109-111.

16. Сивчук Е.С. Социальная инженерия как способ мошенничества // Молодой ученый. – 2020. – № 41(331). – С. 128-130.

17. Осипенко А.Л. Сетевая компьютерная преступность. Теория и практика борьбы: Монография. – Омск: Омская академия МВД России, 2009. – 480 с.

18. Кобец П.Н. Признаки состава преступления и их значение для квалификации преступлений против жизни по российскому законодательству // Научно-исследовательская работа студентов и ее роль в повышении качества учебно-воспитательного процесса: Материалы межвузовской студенческой научно-практической конференции, Москва, 31 мая 2005 года. – Москва: Московский институт права, 2005. – С. 61-72.

19. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 8. – С. 46-50.

20. Кобец П.Н. Механизм передачи осужденных в России иностранных граждан и лиц без гражданства // Деятельность правоохранительных органов и государственной противопожарной службы в современных условиях: проблемы и перспективы развития: 9-я Всероссийская научно-практическая конференция с международным участием, Иркутск, 22–23 апреля 2004 года. – Иркутск: Восточно-Сибирский институт МВД России, 2004. – С. 123-125.

21. Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. Научный журнал. – 2013. – № 5(10). – С. 148-160.

22. Кобец П. Н. Предупреждение экстремизма в России // Актуальные проблемы гуманитарных наук: Сборник научных трудов / Редколлегия: Галкин В.В. - научный редактор, Ильяшенко А.Н., Фефелов В.М., Юрьева И.Ф. - ответственный секретарь. Том Выпуск 1. – Воронеж: Центрально-Черноземное книжное издательство, 2008. – С. 116-118.

23 Колмыков В.В. Уголовно-правовые средства борьбы с преступлениями, совершаемыми в сфере информационных технологий // Современное право. – 2007. – № 9. – С. 20-22.

24. Гладких В.И. Проблемы уголовно-правового регулирования предпринимательской деятельности // Безопасность бизнеса. – 2017. – № 3. – С. 42-47.

25. Кобец П.Н. Современное состояние и перспективы развития профилактики правонарушений в сфере деятельности псевдореволюционных тоталитарных сект и неокультов // Государственная система профилактики правонарушений: современное состояние и перспективы разаития: Материалы межведомственной научно-практической конференции, Москва, 31 октября 2007 года / Министерство внутренних дел Российской Федерации, Всероссийский научно-исследовательский институт. – Москва: Всероссийский научно-исследовательский институт Министерства внутренних дел Российской Федерации, 2008. – С. 447-454.

26. Майоров А.В. Понятие и структура системы противодействия преступности // Правопорядок: история, теория, практика. – 2014. – № 1(2). – С. 112-116.

Шифр специальности: 5.1.4

УДК 343.97

Васькин Денис Александрович
Следователь СО ОМВД России
по Чугуевскому муниципальному округу Приморского края
Россия, Владивосток

Звягин Владимир Андреевич
Начальник кафедры общеправовых дисциплин
Владивостокского филиала Дальневосточного
юридического института МВД России
Россия, Владивосток

Vaskin Denis Alexandrovich
Investigator of the Investigative Department of the Department of Internal Affairs of Russia
in the Chuguevsky municipal district of Primorsky Krai
Russia, Vladivostok

Zvyagin Vladimir Andreevich
Head of the Department of General Legal Disciplines
Vladivostok branch of the Far Eastern
Law Institute of the Ministry of Internal Affairs of Russia
Russia, Vladivostok

Роль потерпевшего при совершении отдельных видов преступлений против собственности

The role of the victim in the commission of certain types of crimes against property

Аннотация: В данной статье рассматривается вопрос виктимного поведения потерпевших при совершении преступлений против собственности. Дается краткая характеристика грабежа, разбоя и вымогательства. Анализируется типология виктимного поведения потерпевших. Реакции потерпевшего при совершении хищения открытым путем. Реакции потерпевшего при совершении вымогательства. Факторы, влияющие на виктимное поведение.
Ключевые слова: преступление, грабеж, разбой, вымогательство, потерпевший, виктимность, реакции потерпевшего.

Annotation: This article deals with the issue of victim behavior of victims when committing crimes against property. A brief description of robbery, assault and extortion is given. The typology of victim behavior of victims is analyzed. The victim's reactions when committing theft in an open way. The victim's reactions when committing extortion. Factors influencing the victim's behavior.
Key words: crime, robbery, extortion, victim, victimhood, victim reactions.

Для виктимологического исследования интерес, имеют такие преступления, как грабеж, разбой и вымогательство. Роль потерпевшего в механизме совершения данных преступлений представляет большое значение для исследования виктимного поведения. В механизме совершения грабежей, разбоя, вымогательства особое место занимает личность потерпевшего. В вышеуказанных преступлениях личность и поведение потерпевшего являются обратной стороной преступления, в которой противоположной стороной является личность преступника. Одним из условий совершения такого рода преступлений является поведение потерпевшего. Для осуществления системного подхода к данному вопросу нужно рассмотреть каждое преступление по отдельности и показать в них проявление виктимного поведения потерпевших.

Разбой представляет собой особую форму хищения, которая заключается в открытом хищении чужого имущества, сопряженного с нападением на жертву [1, с. 501]. Главным фактором в разбои является нападение на потерпевшего, это обстоятельство отличает разбой от кражи или грабежа. Разбой предусматривает использование насилия опасного для жизни или здоровья потерпевшего, а также угрозу применения такого насилия [1, с. 501]. Насилие в вышеуказанном преступлении определяется, как принуждение, применение физической силы или психологического насилия.

Грабеж представляет собой корыстно-насильственное преступление в форме открытого хищения собственности. Грабеж характеризуется признаками, такими как корысть и насилие. Корысть в широком понимании представляет собой стремление к личной выгоде, пользе, наживе. В узком понимании корысть определяется как сознательное стремление к противоправному получению чужого имущество. В упрощенном значении понимание широкой и узкой трактовки сводится к мотиву и цели совершения грабежа [2, с.198]. Особенностью грабежа является то обстоятельство, что данное преступление совершается непосредственно в присутствии потерпевшего либо на виду у посторонних лиц, так как является открытой формой хищения [2, с.198]. Открытый способ хищения свидетельствует о повышенной степени общественной опасности противоправного деяния.

Основываясь на результате обобщения судебной практики можно сделать вывод, что одной из главных задач, стоящих перед преступником в

осуществлении грабежа или разбоя, является подготовка к преступлению путем выбора жертв [3].

Для понимания роли потерпевшего в совершении грабежа или разбоя, имеет значение, как и в какой форме и виде проявляется виктимность в его поведении. К примеру, при совершении хищения открытым путем, как следствие происходящего у потерпевшего могут проявляться следующие реакции:

- испуг, вызванный осознанием реальной опасности, а также неспособность оказать сопротивление преступнику;
- проявление страха, который является следствием логического развития испуга за свое психологическое состояние;
- тревожность, проявляемое как ощущение беспомощности, неуверенности в себе или бессилие перед внешними факторами, то есть в неспособности повлиять на происходящее [2, с.201].

Индивидуальная виктимность, присущая потерпевшим от грабежей и разбойных нападений, складывается из определенных личностных качеств, определяющих недостаточную критичность в оценке опасности. Вышеназванный вид виктимности также выражается в виктимной пассивности или активности потерпевшего и индивидуальных качествах, связанных с особой привлекательностью для преступников в связи с наличием ценного имущества или неспособностью потерпевшего к сопротивлению [2, с. 201].

Для жертв разбойных нападений и грабежей характерно нейтральное, положительное и негативное поведение. Если обратиться к типологии виктимного поведения потерпевших, то вышеуказанные формы поведения относятся к различным типам поведения.

Нейтральное поведение – представляет собой поведение, при котором, лицо своими действиями не способствует возникновению виктимоопасной ситуации, а также такое поведение не связано с неоказанием сопротивления преступнику, если оно объективно возможно [2, с. 201].

Положительное поведение – это осмотрительно и осторожное поведение лица, которое своими действиями не провоцирует преступника на совершение преступления, отличительной чертой которого является оказание сопротивление преступнику [2, с. 201].

Негативное поведение – данное поведение характеризуется действием или бездействием потерпевшего, который создает своими действиями виктимоопасную ситуацию для совершения преступления [2, с. 201]. Примером такого поведения является нахождения потерпевшего в состоянии алкогольного опьянения, как правило, находясь в таком состоянии лицо, плохо ориентируется в обстановке, оказать сопротивление преступнику он также не в состоянии, лицо в таком состоянии может уснуть в каком-либо безлюдном месте, следовательно, стать жертвой грабежа.

Следующим преступлением, представляющим интерес для виктимологического исследования, является вымогательство. Вымогательство представляет корыстно-насильственное преступление, выражающимся в посягательстве на чужое имущество или право на него, способствующее противоправному завладению чужим имуществом [4, с. 23]. Вымогательство одновременно посягает на две группы охраняемых уголовным законом общественным интересов. Это жизнь, здоровье, честь и достоинство, ко второй группе относятся имущественные интересы лица.

Виктимность жертв вымогательства зависит от качеств, которые присуще определенному индивиду, а не группе лиц. В данном преступлении, при определении виктимности поведения потерпевших, нет единых критериев определения поведения жертв вымогательства, для каждого лица они имеют индивидуальный характер. Но, можно выделить ряд качеств присущих жертвам вымогательства, к ним относится низкий уровень правовой культуры, неспособность лица оценить опасность в конкретной ситуации. На предрасположенность потерпевших к виктимному поведению в данном преступлении влияние оказывают ситуативные факторы. Именно вышеперечисленные факторы оказывают влияние на уязвимость потерпевшего. При осуществлении такого преступления как вымогательство, преступник руководствуется данными факторами, выбирает жертву.

Для преступников, осуществляющих вымогательство, привлекательными жертвами являются лица, имеющие в собственности ценный объект или получивший, крупную денежную сумму, имеющим высокий доход, высокий социальный статус. Как правило, к вышеуказанным лицам относятся индивидуальные предприниматели.

С точки зрения виктимного поведения потерпевших от вымогательства, оно делится на нейтральное, позитивное и негативное поведение.

Нейтральное – это такое поведение потерпевшего, которое не оказывает влияние на виктимизацию лица, но при этом такое поведение может причинить вред лицу [4, с. 23]. Преступление здесь возникает не по причине действий потерпевшего, а при обстоятельствах, исключающих возможность распознать опасность преступного посягательства, следовательно, оказать сопротивление преступнику. Такие ситуации возникают при вымогательствах, которые осуществляются на рынках после покупки или у самих продавцов.

Позитивное поведение – это поведение, которое заключается в оказании активного сопротивления преступнику. Оно может, проявляется непосредственно в оказании сопротивления в процессе совершения вымогательства или в обращении в правоохранительные органы.

Негативное поведение – это такое поведение потерпевшего, при котором, он своими действиями способствует совершению против него преступления. Такое поведение потерпевшего делится на активное и

пассивное. При пассивном поведении потерпевший следует и подчиняется требованиям преступника, не уделяя при этом должного внимания охране своего имущества. При активном поведении потерпевший демонстрирует наличие у него богатства ценного имущества, тем самым провоцируя преступника на совершения преступления.

Для эффективной реализации противодействия вышеуказанному преступлению, необходимо выявлять и оказывать предупредительное воздействие на лиц, проявляющих виктимное поведение.

Таким образом, посредством изучения виктимного поведения потерпевшего и понимание его роли в механизме совершения противоправного деяния, встает вопрос о необходимости противодействия вышеназванному поведению. Система противодействия виктимного поведения выражается в проведение профилактических мероприятий, направленных на устранение виктимности в поведение лица. Профилактику виктимного поведения нужно определенным образом структурировать и выработать мероприятия по профилактики каждого вида преступления в отдельности.

Библиографический список:

1. Зотова С.В. Разбой: уголовно-правовая характеристика / С.В. Зотова // Забайкальский государственный университет – 2018. - № 9 – С. 501-509.

2. Окс Л.Е Криминологическая и виктимологическая характеристика грабежа как корыстно-насильственного преступления против собственности / Л.Е. Окс // Общество и право – 2008. - № 2 – С. 198-203.

3. Обзор судебной практики по уголовным делам Верховного суда Российской Федерации 2019 г. (утв. Президиумом Верховного суда РФ 24.04.2019) // Бюллетень Верховного суда РФ – 2019. – № 1.

4. Лечиев Р.С. Криминологическая характеристика вымогательства / Р.С. Лечиев // Научный вестник Омской академии МВД России – 2016. – № 3 - С. 23-27.

УДК 811

Борисенко Ирина Александровна
кандидат филологических наук, доцент
кафедры лингвистики
ФГБОУ ВО «Кубанский государственный медицинский университет»
Россия, г. Краснодар

Бальян Ашхен Мурадовна, кандидат филологических наук, доцент
кафедры лингвистики
ФГБОУ ВО «Кубанский государственный медицинский университет»
Россия, г. Краснодар

Borisenko Irina Aleksandrovna, candidate of philological sciences, associate professor
Department of Linguistics
Federal State Budgetary Educational Institution of Higher Education "Kuban State Medical University"
Russia, Krasnodar

Balyan Ashkhen Muradovna, candidate of philological sciences, associate professor
Department of Linguistics
Federal State Budgetary Educational Institution of Higher Education "Kuban State Medical University" Russia, Krasnodar

К вопросу об использовании некоторых способов и приёмов для запоминания медицинской лексики на занятиях по английскому языку в медицинском университете

On the question of using some methods and techniques for memorizing medical vocabulary in English classes at a medical university

Аннотация: В настоящее время в период глобализации и формирования единого информационного пространства знание иностранного языка считается неотъемлемой частью характеристики высококвалифицированного специалиста. Знание английского языка в современном мире ведет к самосовершенствованию, профессиональному росту и международной активности. Каждый специалист-медик, который занимается научной

деятельностью, должен находится в центре всех новейших достижений в своей сфере. В процессе изучения английского языка студентам приходится заучивать большое количество слов, необходимых для осуществления коммуникативной деятельности. Студенты сталкиваются с необходимостью пополнения и расширения словарного запаса медицинской английской терминологией для работы с профессионально-ориентированными текстами. В данной статье речь идет о способах и приёмах запоминания медицинской лексики, которые могут помочь студентам на занятиях по английскому языку. Этот аспект обучения в медицинском вузе обусловлен необходимостью подготовки высококлассных специалистов, готовых к профессиональному общению. Также в статье рассматриваются такие понятия, как «лексика», «лексические знания» и «медицинская терминология».
Ключевые слова: обучение, английский язык, медицинская терминология, способы, приемы.
Annotation. Nowadays in the period of globalization and formation of a unified information space knowledge of a foreign language is considered an integral part of the characteristics of a highly qualified specialist. Knowledge of English in the modern world leads to self-improvement, professional growth and international activity. Every medical specialist who is engaged in scientific activity should be in the center of all the latest achievements in their field. In the process of learning English students have to memorize a large number of words necessary to carry out communicative activities. Students are faced with the need to replenish and expand their vocabulary with medical English terminology to work with professionally-oriented texts. This article deals with the methods and techniques of memorizing medical vocabulary that can help students in English classes. This aspect of learning in medical university is conditioned by the necessity to prepare highly qualified specialists who are ready for professional communication. The article also considers such concepts as "vocabulary", "lexical knowledge" and "medical terminology".
Key words: learning, English, medical terminology, methods, techniques.

Начиная с XX века, английский язык используется в качестве языка для международного общения. На английском ведутся деловые переговоры, проводятся встречи на высоком уровне, подписываются важные документы.

В настоящее время отмечается быстрое и интенсивное развитие медицинской науки. В соответствие с этим выдвигаются новые цели и задачи к подготовке специалистов-медиков. Знание английского языка способствует повышению уровня молодого специалиста, успеху в карьерном росте, помогает пользоваться зарубежными источниками информации [1].

Обучение языку начинается в школе и продолжается в вузе. Овладение любым иностранным языком – дело сложное и трудоемкое,

которое требует много времени. К моменту поступления в медицинский вуз уровень учащихся оказывается разным: от высокого до нулевого. При поступлении в вуз неязыкового профиля знание английского языка не проверяется, и студенты распределяются в группы произвольно. Поэтому в каждой группе оказываются студенты с разным уровнем знания английского языка.

Современная наука обладает широким спектром разнообразных методов, приемов, технологий в обучении иностранным языкам. При изучении английского языка студентам приходится заучивать большое количество слов, необходимых для осуществления коммуникативной деятельности. Считается, что освоение новой лексики – это самый трудоемкий процесс в изучении иностранного языка. Для этого требуется хорошая память.

Лексика в системе языковых средств является важнейшим компонентом речевой деятельности: аудирования, говорения, чтения и письма. Это определяет ее важное место на каждом занятии по английскому языку.

Лексика (от др.-греч. «относящийся к слову; слово; оборот речи») - словарный состав языка, совокупность слов того или иного языка, части языка [2]. Слова, которые используются в речевой практике человека, как в устной, так и в письменной, составляют его активный словарный запас. Чем богаче и разнообразнее словарный запас человека, тем легче ему пользоваться языком. Лексические знания обеспечивают успешное овладение основами всех видов речевой деятельности. Под лексическими знаниями понимается не только совокупность языковых сведений об иноязычном слове, но и знание программ действия со словом, т.е. определенных стратегий обращения с иноязычным словом [3].

Изучая иностранный язык (английский) в медицинском университете, студентам необходимо пополнять и расширять словарный запас медицинской терминологией на английском языке для работы с профессионально-ориентированными текстами, а также осуществлять коммуникативную деятельность, использовать зарубежные источники информации.

Медицинская терминология - это совокупность слов и словосочетаний, используемых специалистами для обозначения научных понятий в области медицины и здравоохранения [4].

Многие студенты испытывают трудности при изучении английского языка, так как им трудно учить медицинскую лексику на английском, читать и переводить медицинские тексты из-за большого количества новых и сложных английских слов.

При подготовке к занятиям для быстрого и эффективного запоминания медицинских терминов на английском языке, мы рекомендуем студентам использовать следующие методы и приемы:

1.Использование словаря. Изучение новых терминов начинается со словаря.

Словарь — это средство обучения, которое дает определение слову (его значение), ключ к правильному произношению (транскрипция слов, ударение), пополняет запас синонимов и антонимов, показывает то или иное слово в контексте.

Усвоение лексики предполагает выполнение словарной работы. Сейчас широко распространены электронные словари. Их положительной стороной является способность быстрого поиска слова или словосочетания.

2. Использование различных рифмовок

Для запоминания медицинской терминологии мы придумываем разнообразные рифмовки к трудно запоминающимся английским словам. Они облегчают процесс заучивания необходимой лексики, а также развивают способность удерживать в памяти слова и словосочетания. Например, слово blood (кровь) большинство студентов произносят неправильно. Поэтому, следующая рифмовка может хорошо им помочь: blood: cut – part -chart - stud – bud – mud – hud. Или, рифмовка к слову murmur (шум): firmer - termer - sturmer - germer -schermer. При этом словарный запас студентов может существенно пополниться и общеупотребительной лексикой английского языка.

3. Аудиолингвистический метод

При таком методе идет опора на слуховой канал восприятия. Суть метода заключается в многократном прослушивании аудиозаписей или просмотре специальных видеороликов на английском по медицинской тематике. Наиболее эффективным вариантом является просмотр медицинских видеороликов, так как лучше воспринимается материал. Прослушивание аудиозаписей предусматривает воспроизведение вслед за диктором отобранных структур, образцов предложений. Это ведет к их автоматизации.

4. Метод стикеров

Это способ запоминания английских слов, который заключается в наклейке стикеров со словами на предметы, которые они обозначают. Этот метод задействует зрительный канал восприятия. Если при этом еще проговаривать английское слово со стикера вслух, то подключится еще один канал - слуховой.

5. Метод компьютерной техники и сети Интернет

Этот метод является более современным метод обучения. Использование компьютера позволяет формировать графический образ слова одновременно с его звуковым и моторным образом. На занятиях по

английскому языку можно использовать для наглядности презентации, особенно при введении новой лексической темы. Также актуально использовать интернет-ресурсы, как для работы на занятиях, так и при самостоятельной работе студентов.

В заключение хотелось бы отметить, что использование данных методов и приёмов влияет как на успешное усвоение медицинских терминов, так и на отношение студентов к дисциплине «Иностранный язык». Знание и применение медицинской терминологии является необходимой частью профессиональной подготовки студентов медицинского вуза.

Библиографический список:

1.Борисенко И. А., Воднева М. Г. Повышение мотивации и преодоление трудностей при обучении немецкому языку студентов медицинских университетов, Казанская наука, № 10, с. 64-67, 2018г.
2. Кузнецов А. М. Лексика // Лингвистический энциклопедический словарь / Гл. ред. В. Н. Ярцева. — М.: Советская энциклопедия, 1990г.
3. Солтволдиев К. Х. Лексика, лексическая компетентность и лексические знания: обзор / К. Х. Сотволдиев. – Молодой ученый. - № 49 (391), с. 474-475, 2021г.
4. Чернявский М. Н., Дубинина Е. И. Том 25 Большая Медицинская Энциклопедия (БМЭ), под редакцией Петровского Б.В., 3-е издание

НАУЧНОЕ ИЗДАНИЕ

СБОРНИК МАТЕРИАЛОВ

XVIII МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

«Развитие современной науки и технологий в условиях трансформационных процессов» (шифр – МКНТ)

состоявшейся в г. Москва 1 марта 2024 г.

Подписано в печать 15.02.2024г.

Усл. печ. л. 14

mkvrge@mail.ru

www.f-ej.ru