АКТУАЛЬНЫЕ ИССЛЕДОВАНИЯ

МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ

ISSN 2713-1513

#11 (193), 2024

ЧАСТЬ I

Актуальные исследования

Международный научный журнал
2024 • № 11 (193)
Часть I

Издается с ноября 2019 года Выходит еженедельно

ISSN 2713-1513

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

профессор, почетный доктор наук РАЕ, член-корр. Российской академии медико-технических наук (РАМТН) (Астраханский государственный технический университет)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

СОДЕРЖАНИЕ

ТЕХНИЧЕСКИЕ НАУКИ

ВОЕННОЕ ДЕЛО

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

МЕДИЦИНА, ФАРМАЦИЯ

ФИЛОЛОГИЯ, ИНОСТРАННЫЕ ЯЗЫКИ, ЖУРНАЛИСТИКА

КУЛЬТУРОЛОГИЯ, ИСКУССТВОВЕДЕНИЕ, ДИЗАЙН

ПОЛИТОЛОГИЯ

ФИЛОСОФИЯ

ЮРИСПРУДЕНЦИЯ

ТЕХНИЧЕСКИЕ НАУКИ

БЕРЕЗОВ Александр Сергеевич
Россия, г. Москва

ШЛАПАЧЕНКО Игорь Викторович
Россия, г. Москва

РАЗРАБОТКА 3D-ГОЛОГРАФИЧЕСКОГО ПРОЕКТОРА

Аннотация. *Создадим самостоятельно 3D-проектор на базе «Arduin» с целью использования инновации в развитии учебного процесса, применение в медицине, в инженерном плане и маркетинге. Создадим индивидуальную программу для преобразования видео роликов в нужный формат для показа на проекторе.*

Ключевые слова: *3D-проектор, 3D-голограф, голограф, моделирование, проекция, 3D.*

Актуальность работы обусловлена большим сектором применения проектора. На конференциях, презентациях, выставках в наше время очень часто используются 3D-голограммы. Маркетинг и реклама с их помощью успешно привлекают новых клиентов. *В медицине 3D-голограмма нужного органа помогает врачу в деталях увидеть все особенности недуга и исключить ошибку.* При обучении с помощью голограмм можно освоить новый материал как в теории, так и на практике. Сфера развлечений также успешно пользуется этим новшеством: компьютерные игры, шоу-бизнес, ночные клубы. Основное применение это демонстрация макетов, техники и других различных элементов на лекции для увеличения эффективности усваивания материалов.

Чтобы создать 3D-голограмму, необходимо минимум две световые волны. Одна из них является опорной, а другая направляется на объект и называется объектной. В роли волн в современных устройствах используются специальные лазеры, при пересечении которых происходит интерференция, вызывающая трехмерную картинку. Проектор создаёт изображение в результате быстрого вращения, он незаметен для зрителей. С помощью контроллеров вырабатывается серия световых импульсов под крутящийся момент. В результате мы видим яркое трехмерное изображение. Голографический проектор представляет собой устройство, состоящее из тонких лопастей, в которые встроено множество ярких светодиодов RGB высокой плотности. При работе голографического 3D проектора на светодиоды подаются электрические импульсы, синхронизированные с частотой вращения лопастей, в результате чего формируется яркая картинка. Устройство способно транслировать графический и видеоконтент, в качестве которого может выступать логотип, изображение макета, краткие сообщения, другие статические и динамические картинки в рамках рекламной или промокомпании. Контент в голографический 3D проектор можно загружать в файлах большинства популярных форматах через Wi-Fi при помощи мобильного или десктопного приложения. Это же приложение используется для удобного управления устройством. Для того чтобы управлять таким устройством, была разработана индивидуальная программа именно к параметрам этого проектора.

Управление и монтаж: сам голографический проектор может отображать любое изображение, видео или анимацию. Даже обычный. Даже в формате *gif устройство принимает практически любой формат контента, а фактический формат ничем не отличается от обычного монитора/дисплея.

Управление такими устройствами осуществляется через Wi-Fi соединение. Списки воспроизведения создаются с помощью специальных программ проигрывателя. Вы также можете получить доступ и управлять загрузкой

контента удаленно через Интернет и маршрутизатор Wi-Fi.

Конечно, размеры (диаметры) вентиляторов могут быть разными. Наиболее распространенные размеры: 50 см/60 см/65 см/100 см. Диаметр вентилятора равен диаметру самой проекции изображения, мы остановились на 30 см. Установка самого устройства очень простая и быстрая. Это несложно. Стоит беспокоиться только о месте установки. Рекомендуется устанавливать устройство в недоступном для людей месте (если проектор не имеет акрилового защитного кожуха). Следует учитывать, что не все понимают, что такое голографический вентилятор и как он работает. Естественно, многие люди воспринимают 3D-голограммы как воздушные и осязаемые. Как говорится, можно увидеть, но не потрогать. Поэтому особое внимание следует уделить расположению голографических вентиляторов. Например, установить на штатив для камеры и выносить проектор в определённых случаях.

Энергопотребление и автономность: хотелось бы также обратить внимание на низкое энергопотребление таких устройств: для голографического вентилятора диаметром 30 см оно обычно составляет 15–20 Вт. Конечно, все зависит от количества и качества светодиодных диодов. В нашем проекторе использовано 144 диода, энергопотребление составляет 18 Вт. Этот параметр особенно важен, когда требуется низкое энергопотребление.

В других случаях вентилятор может использоваться автономно и, как правило, не имеет доступа к источнику питания. От обычных автомобильных аккумуляторов на 12 В/24 В путем подключения «поворотного столика». Например, мероприятия на открытом воздухе: фестивали, торговые ярмарки и другие места, где нет доступа к сети.

3D контент: Одна из проблем проектора заключалось в том, что он мог показывать видео формат типа bin, но все 3D видео имеют формат типа avi/mp4. Для решения данной проблемы мы разработали специальную программу на языке программирования C++ которая преобразует файлы типа avi/mp4 в формат bin. Эта программа индивидуально имена к нашему проектору так как весь процесс преобразования на прямую зависит от размеров проектора и количество диодов, по итогу мы получаем программу переводящая формат avi/mp4 в круговую диаграмму. Тем самым мы получаем способ демонстрировать любые изображения. После преобразования мы импортируем видео на карту памяти и вставляем в проектор.

Усиление 3D эффекта можно достичь с помощью применения проектора в темном месте и использования рядом с проектором устройство генерирующие дым.

Литература

1. Денесюк Ю.Н. Диссертация об отображение свойств объекта в волновом поле рассеянного им излучения. 1963. 98 с.

2. Ярославский Л.П. Мерзляков Н.С. Цифровая голография. – М.: Наука.1982. 219 с.

BEREZOV Alexander Sergeevich
Russia, Moscow

LOPATCHENKO Igor Viktorovich
Russia, Moscow

DEVELOPMENT OF A 3D HOLOGRAPHIC PROJECTOR

Abstract. *We will create a 3D projector based on Arduino on our own in order to use innovation in the development of the educational process, application in medicine, engineering and marketing. Let's create an individual program to convert video clips to the desired format for display on the projector.*

Keywords: *3D projector, 3D holograph, holograph, modeling, projection, 3D.*

ВАЛИАХМЕТОВ Ильшат Ильдарович
студент, Башкирский государственный аграрный университет, Россия, г. Уфа

Научный руководитель – старший преподаватель кафедры кадастра недвижимости и геодезии Башкирского государственного аграрного университета, старший преподаватель Байков Айдар Гизярович

ИНЖЕНЕРНО-ГЕОДЕЗИЧЕСКИЕ ИЗЫСКАНИЯ ДЛЯ ПРОЕКТИРОВАНИЯ АВТОДОРОГИ

Аннотация. *В статье рассмотрены цель и этапы выполнения инженерно-геодезических изысканий для проектирования автодороги.*

Ключевые слова: *подготовительный этап, полевой этап, камеральный этап, программный комплекс, Публичная Кадастровая Карта.*

Целью данной статьи является рассмотрение процедуры выполнения инженерно-геодезических изысканий.

Для достижения данной цели поставлены следующие задачи:

- изучить законодательную базу, на основе которой выполняется инженерно-геодезические изыскания;
- рассмотреть этапы и особенности изысканий.

Инженерно-геодезические изыскания для строительства проводятся для получения информации о ситуации и рельефе местности, существующих зданий и сооружений и других элементах планировки [2]. Также при создании и ведении государственных кадастров, обеспечения управления территорией, проведения операций с недвижимостью. Правильно составленный топографический план поможет спланировать высоты проектной дороги и их примыкания к существующим дорожным покрытиям. Помимо того топографический план поможет избежать разрушений подземных инженерных сетей при строительстве.

Геодезические работы проводятся в соответствия с требованиями нормативных документов. Система нормативных документов Российской Федерации в строительстве создается в соответствии с новыми экономическими условиями, законодательством и структурой управления на базе действующих в России строительных норм, правил и государственных стандартов в этой области [1].

Геодезические работы делятся на три этапа: подготовительные, полевые и камеральные [3].

В первую очередь подготовительные работы содержат в себе заключение договора с заказчиком и принятие технического задания. На основе технического задания определяется объем выполнения работ и составляется сметная стоимость. Далее производится сбор информации о земельном участке и объекте (получение кадастровой выписки объектов недвижимости; кадастровый план территории; изучение пунктов опорной геодезической сети, расположенных на объекте; картографические материалы и так далее).

В полевом этапе должны быть произведены рекогносцировочные обследования территории, проведения геодезической съемки всех объектов местности (бордюры, существующие постройки, заборы, дорожные покрытия, деревья, откосы и т. д.), а также необходимый объем вычислительных и других работ по предварительной обработке полученных материалов и данных для обеспечения контроля их качества. Особое внимание уделяется обследования на прохождения подземных коммуникации (обследуются колодцы, камеры, проводится поиск трасс с помощью трасоискателей).

На стадии камеральных работ производится обработка полученной информации, уравнивание теодолитных и нивелирных ходов посредством специального программного обеспечения «CredoDat». В программе формируется цифровая модель местности, которая состоит из модели рельефа и ситуации (рис.).

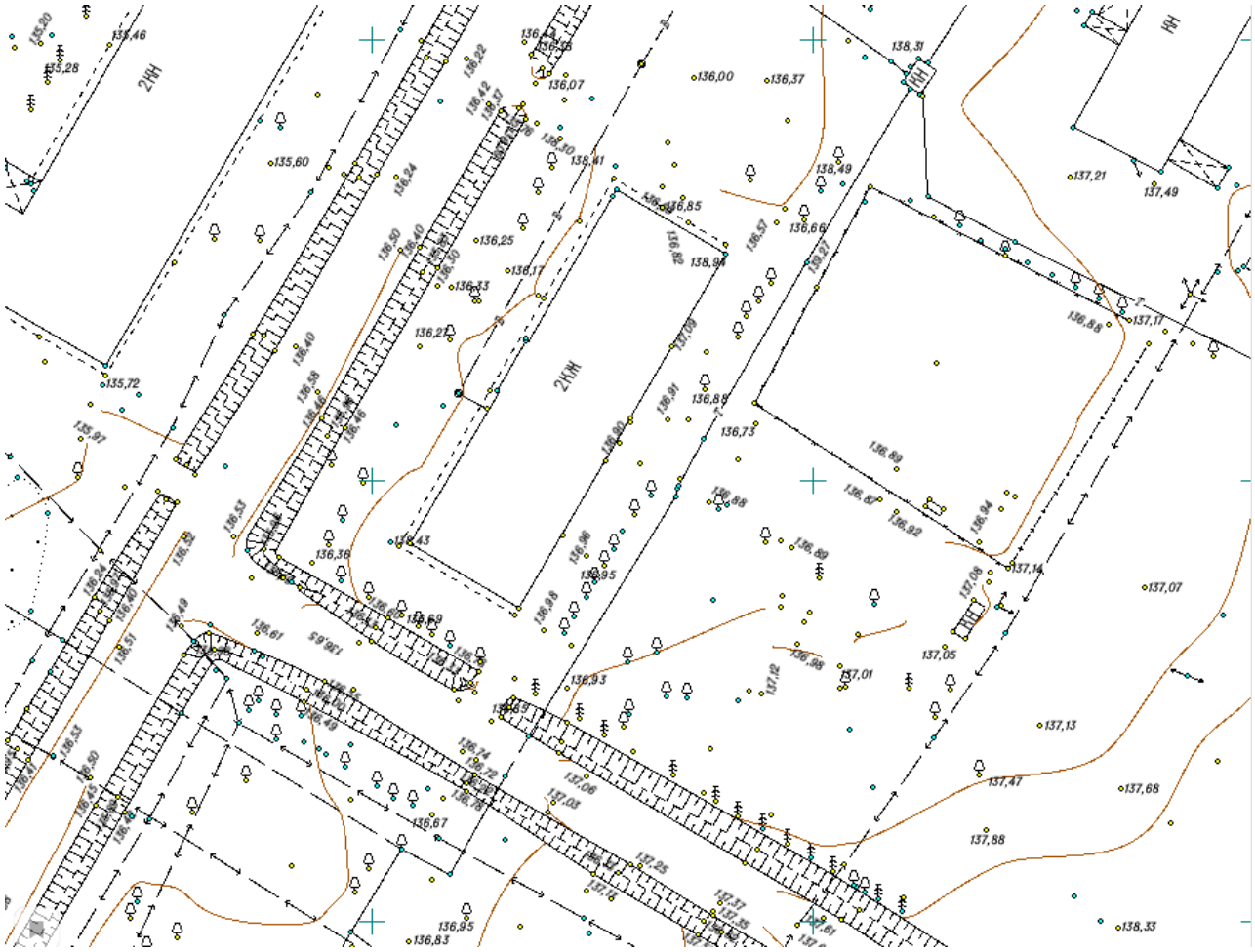


Рис. Цифровая модель местности

Цифровая модель рельефа строится по точкам, полученные с тахеометра методом треугольников строится модель рельефа с точностью до миллиметра. Характерные участки рельефа, такие как хребты, обрывы выделяться структурными линиями.

Цель полевых работ в геодезии – получить точную информацию об объекте с метрическими характеристиками.

После проведения полевых и камеральных работ производится согласования топографического плана на правильность прохождения инженерных коммуникаций. Правильность нанесения подтверждается нанесением соответственной печатью. Заказчику, по окончанию, предается отчет об инженерно-геодезических изысканий и топографический план.

Развитие, применение и установление государственными территориальными фондами материалов инженерных изысканий исполняют в определенной последовательности органы архитектуры и градостроительства исполнительной власти субъектов Российской Федерации или местного самоуправления, а государственным ведомственным фондом материалов комплексных инженерных изысканий – Госстрой России.

Инженерно-геодезические изыскания для строительства выполняются как самостоятельный вид инженерных изысканий и в комплексе с другими видами инженерных изысканий (изыскательских работ и исследований), в том числе инженерно-геологическими, инженерно-гидрометеорологическими и инженерно-экологическими изысканиями, а также изысканиями грунтовых строительных материалов и источников водоснабжения на базе подземных вод.

Вывод: инженерно-геодезические изыскания являются необходимым этапом при строительстве, которые помогут избежать ошибки на этапе проектирования и сэкономить до 40% средств. Помимо того, достоверные данные исключат риск аварийных ситуации.

Литература

1. СНиП 10-01-94 «Система нормативных документов в строительстве. Основные положения».
2. СП 11-104-97 «Инженерно-геодезические изыскания для строительства».
3. Маслов, А.В. Геодезия [Текст]: учебник и учебное пособие для студентов высших учебных заведений / А.В. Маслов, Гордеев А.В., Батраков Ю.Г.– М.: КолосС, 2006. – 598 с.

VALIAKHMETOV Ilshat Ildarovich
Student, Bashkir State Agrarian University, Russia, Ufa

Scientific Advisor – senior lecturer at the Department of Real Estate Cadastre and Geodesy at Bashkir State Agrarian University Baykov Aidar Gizyarovich

ENGINEERING AND GEODETIC SURVEYS FOR ROAD DESIGN

Abstract. *The article discusses the purpose and stages of performing engineering and geodetic surveys for road design.*

Keywords: *preparatory stage, field stage, office stage, software package, Public Cadastral Map.*

ВОЕННОЕ ДЕЛО

БУХМАСТОВ Виталий Владимирович
студент,
Уфимский университет науки и технологий,
Россия, г. Уфа

Научный руководитель – доцент кафедры безопасности производства и промышленной экологии Уфимского университета науки технологий, кандидат технических наук, доцент Нурутдинов Азамат Анварович

ОСНОВНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ ОТ АТАК БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Аннотация. *В данной статье рассматривается проблема защиты потенциально опасных объектов от атак беспилотных летательных аппаратов (БПЛА), с акцентом на FPV-дронах с «машинным зрением». Обсуждаются усовершенствованные системы навигации и сенсоров, которые значительно повышают точность атак и могут обеспечить проникновение в защищенные пространства. Автономность и способность принятия решений на основе собранных данных делают такие дроны менее уязвимыми для активных систем радиоэлектронной борьбы. Также рассматривается классификация БПЛА по размерам и радиусу действия, а также основные типы FPV-дронов и их характеристики. Освещаются трудности обнаружения и противодействия таким дронам, вызванные их маневренностью, использованием различных частот и аналоговых систем передачи видеосигнала.*

Ключевые слова: *беспилотный летательный аппарат, FPV дрон, защита от атак БПЛА, потенциально опасный объект, машинное зрение, противодействие, безопасность, радиоэлектронная борьба.*

В последние годы с развитием технологий беспилотных летательных аппаратов (БПЛА) возникла новая угроза для безопасности потенциально опасных объектов, таких как аэропорты, ядерные электростанции, нефтеперерабатывающие комплексы и прочее. Появление таких аппаратов представляет ряд серьезных проблем для систем безопасности, вызывая необходимость в разработке и внедрении эффективных методов защиты.

Для обеспечения всесторонней безопасности объектов необходимо иметь два ключевых элемента: саму систему защиты и соответствующую нормативно–правовую основу. Согласно законодательным актам Российской Федерации, полеты на беспилотных летательных аппаратах в воздушном пространстве Российской Федерации без разрешения запрещены. Можно сказать, что закон явно относит беспилотники к воздушному судну со всеми вытекающими нормативными требованиями, например, наличие лицензии у пилота и т. п. Все усугубляется тем, что Федеральные правила использования воздушного пространства дают четкое определение Беспилотного летательного аппарата (БПЛА), под которое попадают все радиоуправляемые модели, летающие вне зданий [1, с. 208].

Статья 11.4 части 1 КоАП Российской Федерации за нарушение федеральных правил пользователем воздушного пространства предусматриваются следующие санкции [2, с. 170]:

1. Частным лицам штраф в размере от 2 до 5 тысяч рублей.
2. Должностным лицам штраф от 25 до 30 тысяч рублей.
3. Юридическим лицам штраф от 250 до 300 тысяч рублей.

Дополнительно, с 15 августа 2023 года вступил в силу Федеральный закон от 4 августа 2023

№ 440 –ФЗ [3, с. 3], внесший изменения в Закон Российской Федерации от 11 марта 1992 года № 2487-I «О частной детективной и охранной деятельности в Российской Федерации». Эти изменения предоставляют частным охранным организациям право пресекать работу беспилотных аппаратов, включая воздушные, подводные и надводные суда, а также беспилотные транспортные средства и другие автоматизированные беспилотные комплексы, в рамках предоставления охранных услуг. Эти услуги включают в себя охрану объектов и имущества, а также обеспечение режимов безопасности на объектах, подлежащих обязательным требованиям по антитеррористической защите, за исключением определенных объектов, указанных в законе.

Существует несколько методов разработки стратегий по защите потенциально опасных объектов от беспилотных летательных аппаратов, которые условно можно разделить на пассивные и активные (рис.).

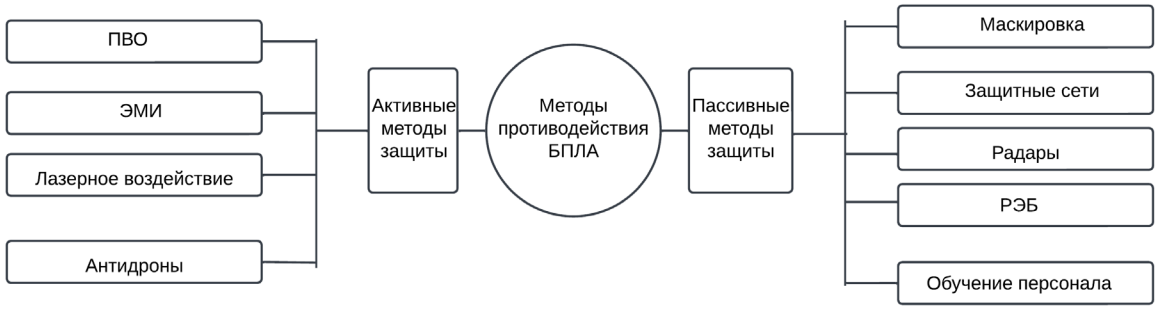


Рис. Методы противодействия БПЛА

Однако современные БЛА начинают обладать усовершенствованными системами навигации, оптическими и радиолокационными сенсорами, что значительно увеличивает точность атак и возможность проникновения в защищенные пространства. Как один из примеров таких БПЛА являются FPV-дроны с «машинным зрением» Комбинация FPV и «машинного зрения» делает эти дроны более автономными и способными воспринимать окружающую среду. Системы радиоэлектронной борьбы (РЭБ) могут столкнуться с рядом технических и тактических трудностей в противодействии FPV–дронам с «машинным зрением». Поскольку FPV-дроны с «машинным зрением» не всегда полагаются на активные радиосигналы для управления. Многие из них могут быть программированы на выполнение предварительно заданных задач или использовать предварительно записанные маршруты. Это делает их менее уязвимыми к активным системам подавления радиосигналов, которые могут блокировать команды от пульта управления. FPV-дроны с «машинным зрением» могут быть способными к автономному принятию решений на основе данных, собранных их сенсорами. Это означает, что они могут продолжать выполнение задач, даже если связь с пультом управления потеряна. В этом случае, даже если системы РЭБ блокируют управляющие сигналы, дрон может сохранять свою работоспособность.

Дополнительно к этому FPV-дроны могут использовать различные частоты для управления и передачи видеосигнала. Это создает трудности для систем РЭБ, которые могут быть настроены на подавление определенных частот, но не всех возможных вариантов использования беспроводной связи дрона. Некоторые FPV-дроны используют аналоговые системы передачи видеосигнала и имеют низкую выходную мощность. Это может затруднять обнаружение и блокирование сигналов дрона с использованием стандартных средств РЭБ. FPV-дроны часто обладают высокой маневренностью и компактными размерами, что делает их сложными для обнаружения и следования за ними в пространстве, особенно при ограниченных средствах РЭБ.

Так Евтушенко Е. В. в своей статье приводит следующую классификацию БПЛА [4, с. 300]:

1. Нано-БЛА: Масса менее 0,025 кг, дальность менее 1 км.
2. Микро-БЛА: Максимальная масса до 5 кг, дальность до 10 км.
3. Мини-БЛА: Дальность до 10 км, масса от 20 до 150 кг.

4. БЛА ближнего радиуса действия: Дальность от 10 до 30 км, масса от 25 до 150 кг.

5. БЛА малого радиуса действия: Дальность от 30 до 70 км, масса от 50 до 250 кг.

6. БЛА среднего радиуса действия: Дальность от 70 до 200 км, масса от 150 до 500 кг.

7. БЛА среднего радиуса действия продолжительного полета: Дальность более 500 км, масса от 500 до 1500 кг.

8. Маловысотные беспилотные аппараты глубокого проникновения: Дальность более 250 км, масса от 250 до 2500 кг.

9. Высотные беспилотные аппараты большой продолжительности полета: Дальность более 2000 км, масса от 2500 до 5000 кг.

Кроме того, существуют специализированные виды беспилотных подводных летательных аппаратов (БПЛА), такие, как ударные, ложные цели, стратосферные, застратосферные и космические БПЛА.

За последнее время наиболее широко используются FPV «дроны» в том числе дооборудованные образцы коммерческого назначения.

Основные типы FPV «дронов»:

1. «Дроны-бомбардировщики» типа «квадрокоптер» предназначены для поражения путем сброса осколочных боеприпасов (ручных гранат типа РГД-5,Ф-1, выстрелов осколочной гранаты ВОГ-17) и кумулятивных боеприпасов (РКГ-3, ПТАБ Mk118 и BLU-77 (США), ПТАБ KB44 DM1244 (Германия), КОБЭ М42/М46 и М77 (США)) за счет попадания в крышу, открытые люки или попаданием в район цели. «Дроны-бомбардировщики» наиболее эффективны против неподвижных объектов.

2. «Дроны-камикадзе» самолетного типа или типа «квадрокоптер», оснащены встроенной кумулятивной или осколочно-фугасной боевой частью (БЧ РПГ ПГ-7Л, ПГ-7М, ПГ-9С, ПГ-18) и предназначены для поражения образцов ВАТ путем попадания (тарана) в верхнюю полусферу цели.

Современные тренды в использовании беспилотных летательных аппаратов для атак на потенциально опасные объекты показывают не только увеличение их эффективности, но и вызывают серьезные вопросы безопасности. Дальнейшее исследование в этой области необходимо для разработки эффективных стратегий обеспечения безопасности промышленных объектов и регулирования использования БПЛА в военных целях.

Литература

1. Винокурова В.В., Вытовтов А.В., Шумилин В.В. Административно правовое регулирование использования беспилотных летательных аппаратов в Российской Федерации // Проблемы обеспечения безопасности при ликвидации последствий чрезвычайных ситуаций. 2015. № 1. С. 207-217.

2. Кодекс Российской Федерации об административных правонарушениях № 195. 2001, Российская газета. 635 с.

3. Федеральный закон № 440 «О внесении изменений в отдельные законодательные акты Российской Федерации». Парламентская газета. 2021, 23 с.

4. Евтушенко Е.В., Володин А.Н. Анализ существующих типов беспилотных летательных аппаратов и перспектив их развития // Интеллектуальные системы, управление и мехатроника. 2017. С. 299-305.

BUKHMASTOV Vitaliy Vladimirovich
Student, Ufa Institute of Science and Technology,
Russia, Ufa

Scientific Advisor – Associate Professor of the Department of Industrial Safety and Environmental Engineering of the Ufa Institute of Science and Technology, Ph.D., Associate Professor Nurutdinov Azamat Anvarovich

MAIN PROBLEMS OF PROTECTING POTENTIALLY DANGEROUS OBJECTS FROM UNMANNED AERIAL VEHICLE ATTACKS

Abstract. *This article addresses the problem of protecting potentially dangerous objects from unmanned aerial vehicle (UAV) attacks, with a focus on FPV drones with "machine vision." Advanced navigation and sensor systems are discussed, which significantly increase the accuracy of attacks and may enable penetration into protected spaces. Autonomy and the ability to make decisions based on collected data make such drones less vulnerable to active electronic warfare systems. Also considered is the classification of UAVs by size and range, as well as the main types of FPV drones and their characteristics. The difficulties of detecting and countering such drones are highlighted, stemming from their maneuverability, use of various frequencies, and analog video transmission systems.*

Keywords: *unmanned aerial vehicle, FPV drone, protection against UAV attacks, potentially dangerous object, machine vision, countermeasures, security, electronic warfare.*

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

SHASHENKO Alisa Andreevna
Student, Institute of Information Technologies, Sevastopol State University,
Russia, Sevastopol

PIROGOV Eduard Ruslanovich
Student, Institute of Information Technologies, Sevastopol State University,
Russia, Sevastopol

Scientific Advisor – Associate Professor of the Department of Foreign Languages of Sevastopol State University, Candidate of Philology, Associate Professor Ivantsova Julia Alexandrovna

RATIONALE FOR A NEW APPROACH TO POST-QUANTUM ENCRYPTION

Abstract. *The article examines the existing encryption algorithms, during which it becomes clear that none of them can provide reliable encryption in cases where a hacker attack is conducted using quantum computers. To solve this problem, a new method has been proposed that combines both symmetric and asymmetric encryption in such a way that symmetric keys are generated on both the server and the client according to the general rule for each new message. In this case, a message is an HTTP request. This approach increases the total hacking time in proportion to the number of incoming messages to the information system. For example, it takes 19 hours to hack a system that is protected by the HTTPS protocol using a quantum computer with 1,282 qubits. And the proposed method will multiply this time by the number of all messages. From this it becomes clear that this is an extremely effective method. Moreover, this method can be used in conjunction with HTTPS to make encryption even more reliable. This combination becomes possible due to the fact that the proposed method operates at the application level, while HTTPS operates at the protocol level. That is, both methods can function simultaneously, complementing each other. With this approach, hackers will first need to crack the private key of the SSL certificate, after which they will start hacking the set of keys generated using the proposed method.*

Keywords: *encryption, quantum computing, symmetric encryption, asymmetric encryption, post-quantum encryption, information security.*

In today's world, we often need to transmit sensitive information over the internet. This can include passwords, personal data, and other confidential information that should never be accessed by third parties. Unfortunately, in 2019, there were 11,000 reported cases of personal data leaks in Russia, which is a 27% increase from the previous year. The average fine for violating personal data laws in Russia was 75,000 rubles in 2019. Rosstat [1] reported 1,087 information technology and communications-related crimes in 2020, with 1,017 of them involving unauthorized access to computer information.

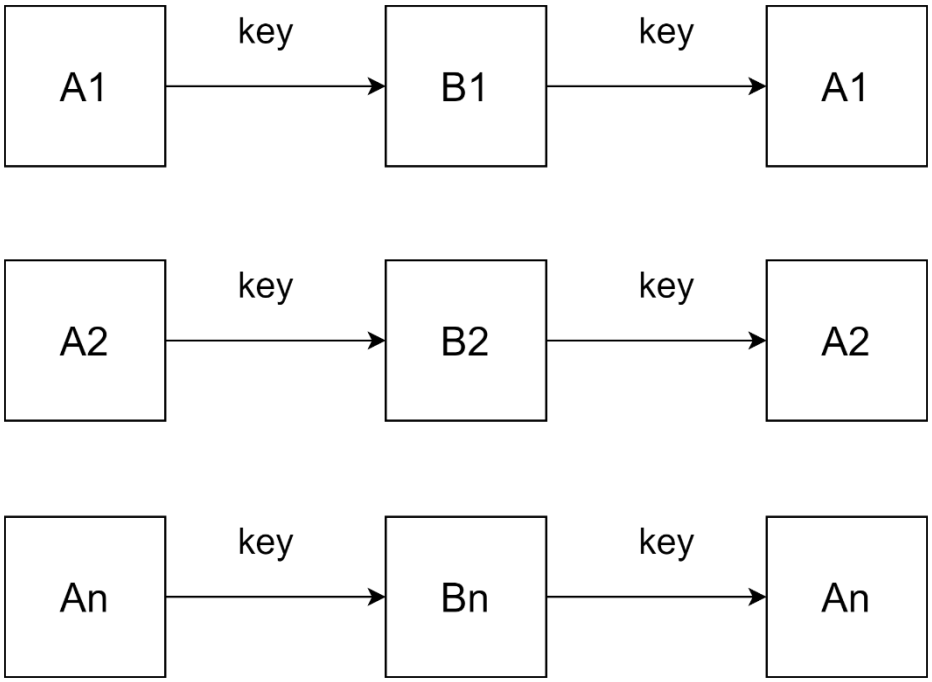
This statistic may worsen as quantum computers become more prevalent. These computers perform electronic calculations much faster than conventional and supercomputers because they use three values (0, 1, and superposition) instead of two. Existing encryption methods need modification as they can no longer ensure information system security in their usual form. Before the advent of quantum computers, it was rational to use the same key to encrypt all messages in symmetric encryption. This was due to the fact that with this approach it was not necessary to exchange keys often, and hacking one such key using a conventional computer in a reasonable time was practically impossible for technical reasons: it required too much processor time and large amounts of Random-Access Memory (RAM) to sort through all

possible combinations. However, the problems with processor time and storage of large amounts of data are not so acute for a quantum computer.

Thus, it becomes obvious that today the problem of information protection is quite urgent, therefore it is necessary to invent new encryption methods and modify existing ones, combining them to resist hackers who can use quantum computers for fast calculations.

To understand which method and how exactly it can be modified or combined, existing encryption methods and some post-quantum modifications of asymmetric encryption were reviewed and analyzed in detail.

For example, there is symmetric encryption. Symmetric algorithms provide high-speed encryption and decryption of data, since they use the same key for both operations [2, p. 74-78; 3; 4, p. 18-20], which means that only one key needs to be generated, and not, for example, a pair of keys, as happens with asymmetric encryption. In addition, the speed is achieved due to the fact that a symmetric encryption key usually has a relatively small length: from 128 to 256 bits [5, p. 164-167; 6, p. 6-9; 7, p. 30-31]. This makes it possible to process large amounts of information with minimal delays and overhead of processor time [8, p. 82-87]. The essence of symmetric encryption methods is to bring the message A_n to the form B_n on the sending side using a passphrase, and on the receiving side using a passphrase to bring the message B_n to the form A_n (pic. 1).



Pic. 1. The scheme of operation of the symmetric encryption algorithm

It is important to understand that the key is generated based on some keywords. In fact, it's just a set of characters, that is, a string, for example, "A keyword with complex characters &^* and numbers 123943, which is extremely difficult to crack by brute force." The longer the sequence of characters in a keyword, the better, because the more difficult it will be to find it by brute force. In this case, the key itself is a sequence of bits from 128 to 256 in length, depending on the specific encryption algorithm. The message A_n can also be anything, for example, a string "I love science." In this case, the message B_n is a sequence of characters incomprehensible to humans [9, p. 20-23], for example, "U2FsdGVkX1+WDKb95q2", which cannot be understood without decryption using the passphrase that was used for encryption on the sending side. The symmetric encryption process can be formalized as follows: imagine E_k as some encryption operator for which the following statement is true:

$$E_k = M \overset{k}{\rightarrow} C, \quad (1)$$

where M is plaintext, C is private text, and k is the encryption key. That is, E_k maps plaintext to private text using the k key. Then the formula for the set of encrypted messages using symmetric encryption can be written as

$$O = \overset{N}{\underset{i=1}{U}} C_i, \quad (2)$$

where O is the set of encrypted messages of some information system, N is the number of messages,

C_i is an encrypted message (closed text) that was encrypted using the E_k operator.

Although this approach may seem promising, symmetric encryption algorithms pose a risk of compromising the key phrase. This phrase is distributed between conversation participants through various communication channels [10, p. 3-33]. Furthermore, this approach ensures that all messaging participants use the same key, simplifying the process of hacking. Only one key needs to be hacked, for example, through brute force, to decrypt all correspondence at once. The primary issue with hacking is that it can go undetected due to the lack of tracking tools. Unless the attacker reveals themselves by publicly using decrypted information, it is difficult to detect. However, from the hacker's perspective, it is more prudent to continue monitoring the communication channel after obtaining the secret key, rather than revealing themselves.

Therefore, it is evident that the use of symmetric encryption in its classical form is no longer rational with the emergence of quantum computers. This is due to the unreliability of communication channels and the need for frequent key changes.

To solve the problem of key compromise, an asymmetric encryption method has emerged based on the use of two keys: public and private. This method assumes that the private key is kept strictly confidential and is not shared among the conversation participants, while the public key is distributed to all participants. Asymmetric encryption algorithms utilize a private key exclusively for decrypting messages that have been encrypted using the corresponding public key. The process can be summarized as follows: Interlocutor A provides Interlocutor B with public key X. Interlocutor B uses key X to encrypt message M and sends the encrypted message MS to Interlocutor A. Interlocutor A decodes MS using private key Y to receive the original message M. Therefore, it is evident that this approach is superior to symmetric encryption. Each party possesses their own private key (Y), and the public key (X) can be safely transmitted over unsecured communication channels. This is because third-party interception of the public key does not pose any threat. It is important to note that the public key can only be used to encrypt a message, not decrypt it. The above reasoning explains the following formulas more clearly:

$$E_{k_{open}} = M \xrightarrow{k_{open}} C, \quad (3)$$

$$D_{k_{private}} = C \xrightarrow{k_{private}} M, \quad (4)$$

where $E_{k_{open}}$ is the asymmetric encryption operator, k_{open} is the public encryption key, $k_{private}$ is the private key, C is the encrypted message, M is the original message, $D_{k_{private}}$ is the asymmetric encryption decryption operator. Based on this, it becomes clear that the public key is used only for encryption, and the private key is used for decryption. In this regard, using an asymmetric encryption method is a more secure solution than using symmetric encryption algorithms.

However, this approach also has vulnerabilities. For instance, although it was previously believed that the public key could be sent without fear of interception, the advent of quantum computers has rendered the asymmetric encryption method, known as RSA, vulnerable to attacks. This is due to the Shore algorithm, which can be used to obtain a private key from a public key by solving the problem of finding prime factors of an integer.

In this regard, asymmetric encryption algorithms have been developed that are resistant to quantum computing. Among these, CRYSTALS-Dilithium, FALCON and SPHINCS+ can be distinguished, the essence of which is to use cryptographic methods based on solving problems of lattice theory or hash functions, the solution time of which does not differ on conventional and quantum computers. This is very reasonable, since Shore's algorithm cannot be applied to either lattice theory or hash functions.

However, the problem has not disappeared worldwide: the public key is still transmitted carelessly over open communication channels in the hope that it will not be possible to obtain the private key, but it is only a matter of time before an algorithm appears that can solve the problem of lattice theory or even hash functions. This is particularly relevant in the current era of rapid artificial intelligence development.

It is also important to note that asymmetric encryption is not a complete solution to the problem of information security, for the sole reason that asymmetric encryption is several orders of magnitude slower than symmetric encryption due to the longer encryption keys. Looking at the problem in more detail, it becomes clear that asymmetric encryption should be used as rarely as possible and only for specific purposes, such as transferring symmetric encryption keys.

Thus, it is obvious that existing encryption methods, including those considered to be resistant to quantum computers, do not allow reliable encryption of data transmitted via the Internet. In this regard, it seems relevant to formulate the

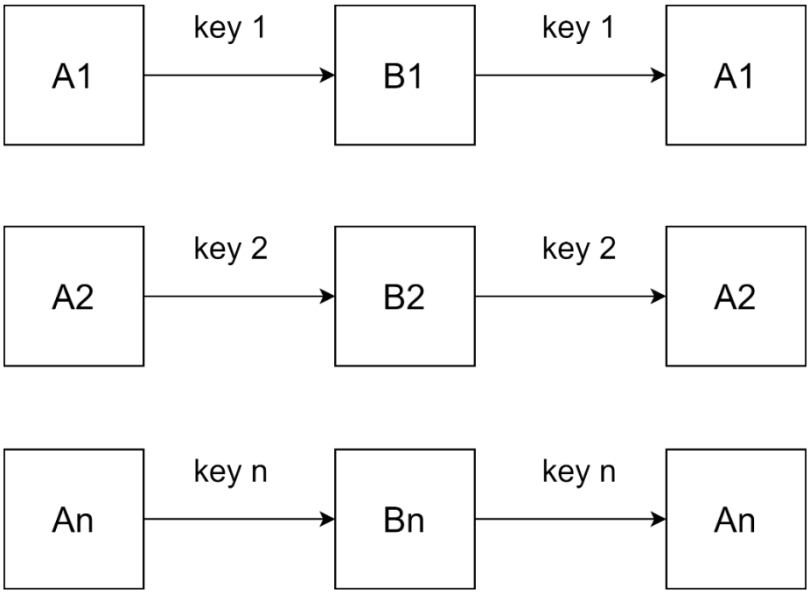
task of developing such a method of information protection that will not have weak points or will have a minimum number of them and will ensure reliable encryption of information even in cases when a hacker attack is carried out using quantum computers.

A post-quantum encryption method has been proposed that does not include a public key, which makes it more secure against quantum attacks than asymmetric methods. For a more detailed consideration, it is necessary to introduce the following concepts:

- A message is a GET or POST request for the HTTP protocol.
- A client is a wrapper for an HTTP client that allows you to send HTTP requests using a user-friendly UI, that is, it can be a website or a mobile or desktop application.
- A server is a web application that accepts HTTP requests, processes them, and returns a response to incoming requests.

The essence of the method is to modify the symmetric encryption method. This modification proposes generating a new encryption key for each message, rather than using a single key for all messages. Each key can only encrypt and decrypt one message. Additionally, the encryption key must be generated using the same rule on both the client and server to avoid the need to send the key over communication channels.

In general, the modification of symmetric encryption has the form shown in Pic. 2. Here A_1, A_2, ... A_n is the original message, B_1, B_2, ... B_n is the encrypted form of the original message. In turn, key 1, key 2, ... key n is the key for message n.



Pic. 2. The scheme of operation of the symmetric encryption algorithm

The formula for the set of encrypted messages of the symmetric encryption modification will have exactly the same form as formula (2) with one difference – each message uses its own k_i key to encrypt, that is, the operator is used:

$$E_{k_i}: M_i \overset{k_i}{\rightarrow} C_i \quad (5)$$

It is obvious that even if $M_1 = M_2 = M_n$, then $C_1 \neq C_2 \neq C_n$, because $k_1 \neq k_2 \neq k_n$.

For a more detailed understanding of the operation of this method, it is rational to consider a text messaging system that provides communication between users of the system, that is, a kind of messenger. The classic version of symmetric encryption involves creating an encryption key on the server and transmitting it to all system participants, i.e., clients. It becomes obvious that with this approach, two problems appear at once: first, the key can be intercepted at the moment of its transfer to clients; Secondly, a hacker needs to crack just one key, which is not a big problem if a quantum computer is used.

While the modification of symmetric encryption solves both of these problems, because the modification assumes that both the client and the server know how to generate the encryption key, which means that there is no need to transmit it over communication channels. Moreover, even if some key is hacked by brute force, the benefit from this from the hacker's point of view will be minimal, because this key will be able to decrypt only

one message, which means it will be useless for other messages.

It was previously observed that the key is generated from a string keyword, allowing for a great deal of flexibility as the string can be generated based on a set of rules. For example, you can use the current time in the format "current day.current.month.the current year.the current hour. the current minute." Obviously, according to this rule, you can create a string on both the client and the server, because both of them can find out the current date and time.

Consider this example: User A wants to send a message to User B that includes a quote from Mikhail Vasilyevich Lomonosov: 'Mathematics should be studied because it puts the mind in order.' When User A clicks the 'Send message' button, the client application must create a keyword based on the aforementioned rule, receive a key, encrypt the message with this key, and transmit it to the server using HTTP or HTTPS protocol. Upon receiving the encrypted message, the server must generate a keyword using the same rule as the client, which takes into account the time to the minute.

In some cases, messages may be delayed due to prolonged communication channels. To address this issue, the program code can undergo various checks. So, for example, if it was not possible to decrypt the message according to the above rule, then you can try using the following rule: "the current day.the current month.the current year.the current hour. the previous minute." Similarly, we can assume that the message was sent at 12:59, and arrived on the server at 13:00, so the following rule should be provided: "the current day.the current month.the current year.the previous hour is 00." In addition, the message can be sent, for example, in 2023, and come to the server in 2024, for this you also need to provide a rule: "31.12.the previous year.23.59".

While this approach may appear reliable, it has a significant flaw. If any encryption key is compromised, all messages sent during that time period can be decrypted. Additionally, if a hacker studies the application's source code, hacking becomes an easy task. To mitigate these issues, it is recommended to personalize the keyword formation rule by adding unique information to messages generated for each user.

To do this, you can implement such a request on the server, which will return, for example, 10,000 random characters, which will be transmitted to the client using asymmetric encryption. At the moment, it is more reliable to use a post-quantum asymmetric method, for example, CRYSTALS-Dilithium, since it is invulnerable to the Shore algorithm. These 10,000 characters can be used to generate a keyword, for example, as follows: "10,000 characters. The current day. The current month. The current day. The current hour. The current minute."

Thus, each user will have a unique key even if the same date and time were used to generate it. This approach makes the algorithm invulnerable to hackers who know the source code of the software product. An attacker may see that the keyword is generated using the current date and time, but they will not be able to determine the 10,000 characters that precede the date and time.

Therefore, modifying symmetric encryption enhances security. Even if a secret key is selected through brute force, only one message can be decrypted.

It is important to note that this modification of symmetric encryption has the advantage that the software developer can implement the algorithm independently, improving security and performance by allowing for selective encryption. For instance, consider a scenario where a user is requested to vote in an anonymous poll. The POST request would contain a unique survey ID and the number of the selected item. The message does not provide useful information to a potential hacker as it does not disclose the corresponding survey for this unique identifier. This information is classified and only accessible to the developer with database access. Therefore, encrypting this request is unnecessary. This can significantly improve performance for frequent or similar queries, particularly in mobile applications where it can also save battery power.

When considering this method, it is important to evaluate its effectiveness in comparison to other existing methods. For example, conventional symmetric encryption without constantly changing the encryption key and asymmetric encryption is both viable alternatives. The calculations used hypothetically possible hacker attacks as it would be too time-consuming to implement such testing in practice. Additionally, quantum computing was not considered due to its lack of availability at the time of the study.

A comparison was conducted on the time it takes to hack systems that implement different types of encryption: symmetric encryption with a 256-bit encryption key, asymmetric encryption with a 2048-bit encryption key, and the method proposed in this study (referred to as 'modification of symmetric encryption') with 256-bit encryption keys. The text describes two scenarios for hacking: using the Fugaku supercomputer, currently the most powerful in the world, and using a quantum computer. The calculations are designed to produce results within hours.

The performance of the Fugaku supercomputer is 442 petaflops. This means that it is capable of performing $442 \cdot 10^{15}$ operations per second. Based on this information, it can be concluded that this supercomputer is able to crack a symmetric 256-bit encryption key in:

$$\frac{2^{256}}{442 \cdot 10^{15} \cdot 3600} \approx 7 \cdot 10^{55} \quad (6)$$

hours. This number is greater than a billion years and even exceeds the age of the universe. This formula is explained as follows: the encryption key has a length of 256 bits, and the bit, in turn, can take one of two values: 1 or 0, which is why 2^{256} is written in the numerators, that is, one of two values can be in each of the 256 positions. The denominator records the number of operations that the Fugaku supercomputer is capable of performing in one second. This number was multiplied by 3600 to get the answer not in seconds, but in hours. That is, in general, this formula can be written as follows:

$$\frac{2^d}{k}, \quad (7)$$

where d is the key length in bits, k is the number of operations per second. With asymmetric encryption, at the time of writing, it is customary to use a key with a length of 2048 bits, which means that a supercomputer will need to crack such a key:

$$\frac{2^{2048}}{442 \cdot 10^{15} \cdot 3600} \approx 2 \cdot 10^{595} \quad (8)$$

hours. This number is also quite large; however, a quantum computer is able to decrypt much faster. For example, to crack a symmetric encryption key, a quantum computer with 150 qubits will only need:

$$\frac{2^{256}}{3^{150} \cdot 3600} \approx 86 \quad (9)$$

hours, which is about 3.5 days. This is still a large number, but this time can be considered quite reasonable, given the benefits that the hacker will receive. It is worth noting that the decryption rate with this approach increases in proportion to the number of qubits. For example, even with 160 qubits, a quantum computer is able to crack a 256-bit key in just 5 seconds. It is worth paying attention to the denominator in this formula. The number 3^{150} means that 150 qubits are used, and each qubit can be in one of three states: in addition to 1 and 0, it can be in a superposition state. That is, in general, the formula can be written as follows:

$$\frac{2^d}{3^k}, \quad (10)$$

where d is the key length in bits, k is the number of qubits. Accordingly, to crack the encryption key with a length of 2048 bits, a quantum computer will need:

$$\frac{2^{2048}}{3^{1282} \cdot 3600} \approx 19 \quad (11)$$

hours if 1282 qubits are used. However, even if there are 1290 qubits, such a key will be cracked in just 10.5 seconds.

It is evident that a quantum computer presents a significant threat to encryption keys of any size. This is because the number of qubits compensates for the length of the encryption key.

The use of symmetric encryption has been modified to significantly slow down the hacking process. This is achieved by multiplying the numerator by N, where N is the number of messages that need to be decrypted, in both the formula for cracking a 256-bit symmetric encryption key on a supercomputer and the formula for hacking on a quantum computer. Considering the potential volume of messages, such as hundreds of thousands per day, hacking would be considerably challenging even on a quantum computer with a high number of qubits. Thus, the Fugaku supercomputer will need:

$$\frac{2^{256}}{442 \cdot 10^{15} \cdot 3600} \cdot N \approx 7 \cdot 10^{55} \cdot N \quad (12)$$

hours to crack all messages of an information system implementing a modification of a symmetric encryption algorithm. A quantum computer will need hours. And this is a pretty tangible result.

$$\frac{2^{256}}{3^{150} \cdot 3600} \cdot N \approx 86 \cdot N \quad (13)$$

Table shows the calculations mentioned earlier. The column 'Time spent hacking on a computer in hours' assumes that a computer refers to a Fugaku supercomputer.

Table

Comparison of hacking time for systems using different types of encryption

The name of the algorithm	Computer hacking time in hours	The time to hack a quantum computer in hours
Symmetric encryption	$\frac{2^{256}}{442 \cdot 10^{15} \cdot 3600} \approx 7 \cdot 10^{55}$	$\frac{2^{256}}{3^{150} \cdot 3600} \approx 86$
Asymmetric encryption	$\frac{2^{2048}}{442 \cdot 10^{15} \cdot 3600} \approx 2 \cdot 10^{595}$	$\frac{2^{2048}}{3^{1282} \cdot 3600} \approx 19$
Modification of symmetric encryption	$\frac{2^{256} \cdot N}{442 \cdot 10^{15} \cdot 3600} \approx 7 \cdot 10^{55} \cdot N$	$\frac{2^{256} \cdot N}{3^{150} \cdot 3600} \approx 86 \cdot N$

In conclusion, current methods offer a good level of protection against conventional computers and supercomputers, but they are vulnerable to quantum computers, which are able to crack encryption keys in a reasonable time. However, the modification of symmetric encryption proposed in this study offers much greater security than the use of symmetric encryption in its classical form, since the time taken to hack the entire information system is directly proportional to the number of messages, which can increase by millions every day if we are talking about a large social network, for example.

Based on the information received, a second conclusion can be drawn: a quantum computer with enough qubits can crack encryption keys in seconds, regardless of their length. However, the study suggests that there is still a significant amount of time before this becomes a reality. However, the proposed modification of symmetric encryption will only be effective until quantum computers become widely available with more than 150 qubits.

This study may also inspire other researchers to consider ways to protect against quantum computers with thousands of qubits.

Литература

1. Росстат. Официальная статистика. – Режим доступа: https://rosstat.gov.ru/folder/10705. (Дата обращения: 29.04.2023).

2. Берников В.О. Сравнительный анализ криптостойкости симметричных алгоритмов шифрования // Труды БГТУ. Серия 3: Физико-математические науки и информатика. 2020. № 1 (230). С. 74-78.

3. Бабенко Л.К., Ищукова Е.А. Криптографическая защита информации: симметричное шифрование // Учебное пособие / Сер. 11 университеты России (1-е изд.) Москва, 2018.

4. Горелик В.Ю., Трифонов Д.И., Матвеев М.В. Алгоритмы симметричного блочного шифрования // Автоматика, связь, информатика. 2019. № 11. С. 18-20.

5. Кочкаров Э.Р. Описание симметричного алгоритма блочного шифрования AES-128 // Тенденции развития науки: инновационный подход. Сборник материалов Международной научно-практической конференции. 2019. С. 164-167.

6. Шуваев В.В. Сквозное (оконечное) шифрование // Молодой учёный. 2019. № 6 (244). С. 6-9.

7. Чичикин Г.Я., Семёнов Д.А. Сквозное шифрование // Academy. 2019. № 5 (44). С. 30-31.

8. Алексеев К.А., Карнаухов Е.В., Сливинский В.Д. Сквозное шифрование и его применение в мессенджерах // Вопросы контроля хозяйственной деятельности и финансового аудита, национальной безопасности, системного анализа и управления. сборник материалов III Всероссийской научно-практической конференции. ФГБНУ «Аналитический центр» Минобрнауки России. 2018. С. 82-87.

9. Шабала М.Д. Исследование модификаций симметричного алгоритма блочного шифрования AES // Молодёжная научная школа кафедры «Защищённые системы связи». 2020. Т. 1. № 2 (2). С. 20-23.

10. Al-Riyami S., Paterson K. Certificateless Public Key Cryptography // Advances in Cryptology - ASIACRYPT 2019. Lecture Notes in Computer Science. 2019. Vol. 11921. P. 3-33.

ШАШЕНКО Алиса Андреевна
студентка, Институт информационных технологий,
Севастопольский государственный университет, Россия, г. Севастополь

ПИРОГОВ Эдуард Русланович
студент, Институт информационных технологий,
Севастопольский государственный университет, Россия, г. Севастополь

Научный руководитель – доцент кафедры иностранные языки
Севастопольского государственного университета, канд. фил. наук, доцент
Иванцова Юлия Александровна

ОБОСНОВАНИЕ НОВОГО ПОДХОДА К ПОСТКВАНТОВОМУ ШИФРОВАНИЮ

Аннотация. *В статье рассматриваются существующие алгоритмы шифрования, в ходе чего становится ясно, что ни один из них не может обеспечить надёжное шифрование в случаях, когда хакерская атака ведётся с использованием квантовых компьютеров. Для решения этой проблемы был предложен новый метод, который комбинирует как симметричное, так и асимметричное шифрование таким образом, что как на сервер, так и на клиенте симметричные ключи генерируются по общему правилу для каждого нового сообщения. Под сообщением в данном случае понимается HTTP запрос. Такой подход увеличивает общее время взлома пропорционально количеству поступающих сообщений в информационную систему. Так, например, для взлома системы, которая защищена протоколом HTTPS требуется 19 часов с помощью использования квантового компьютера, имеющего 1282 кубита. А предложенный метод умножит это время на количество всех сообщений. Из этого становится ясно, что это крайне эффективный метод. Более того, данный метод можно применять совместно с HTTPS, чтобы сделать шифрование ещё более надёжным. Такая комбинация становится возможной благодаря тому, что предложенный метод функционирует на уровне приложения, в то время как HTTPS – на уровне протокола. То есть оба метода могут функционировать одновременно, дополняя друг друга. При таком подходе хакерам нужно будет сначала взломать приватный ключ SSL сертификата, после чего приняться взламывать множество ключей, генерируемый при помощи предложенного метода.*

Ключевые слова: *шифрование, квантовые вычисления, симметричное шифрование, постквантовое шифрование, защита информации.*

ГЕРАСИМОВ Андрей Сергеевич
генеральный директор, ООО «Диджитал Групп»,
Россия, г. Москва

БЕЗОПАСНОСТЬ В ОРГАНИЗАЦИИ

Аннотация. *Любое государственное, либо частное предприятие обязано надежно и эффективно обеспечивать информационную безопасность. Это очень важно, т. к. технологии постоянно развиваются, а сфера применения компьютеров и другого оборудования расширяется. Цели ИБ формируют, исходя из задач, которые стоят перед системой кибербезопасности отдельной компании. Чем важнее данные, тем больше они нуждаются в защите. Постоянно развивающиеся инструменты ИБ отслеживают любые изменения в системном коде и попытки несанкционированного проникновения в хранилище информации. Если уделять кибербезопасности мало времени и средств, то могут нагрянуть катастрофические последствия в виде утери важных сведений, заражения вредоносными кодами, неправомерного доступа посторонних лиц к банку данных и т. д. Главная задача ИБ – максимально ограничить подобные ситуации и предусмотреть все потенциальные опасности. Чем выше надежность системы, тем ниже вероятность взлома.*

Ключевые слова: *информационная безопасность (ИБ) в организации, защита информации, система физической защиты, аппаратные средства защиты, программные средства защиты.*

Основная часть

Мировой прогресс в информационном обеспечении ставит новые задачи не только перед государствами, но и субъектами экономики страны в защите своего информационного пространства от несанкционированного доступа. Усиливается роль служб информационного обеспечения организации, проводятся работы по анализу уязвимости каналов связи. Все эти явления обуславливают актуальность информационной безопасности в организации [1].

Данные необходимо защищать везде – от ресурсов отдельных пользователей до порталов государственного уровня. Кроме непосредственного обеспечения безопасности, нужно предоставлять каждому юзеру качественную и достоверную информацию, а также оказывать правовую поддержку при работе со сведениями. Поэтому главная цель ИБ – сформировать условия, которые обеспечат высококачественную и эффективную защиту важных данных от намеренного либо случайного вмешательства, ведь такое вмешательство способно повредить, удалить, изменить или другим способом воздействовать на конфиденциальные сведения.

Угрозы безопасности разделяют на две категории: внутренние и внешние.

Внутренние. Это угрозы, которые идут изнутри системы. Чаще всего в таких случаях речь идет об утечке данных или об их повреждении. Например, кто-то подкупил сотрудника, и тот похитил данные, составляющие коммерческую тайну. Второй вариант – злоумышленником оказался авторизованный пользователь.

Еще одна внутренняя угроза – риск банальной ошибки, в результате которой конфиденциальные сведения окажутся в открытом доступе или повредятся. Например, в открытом доступе оказалась часть базы данных или пользователь по неосторожности повредил файлы. Такое уже бывало в истории. А нужно, чтобы таких случаев не возникало: клиент не мог бы нарушить работу системы даже случайно, а информация оставалась защищена.

Внешние. Сюда относятся угрозы, которые приходят извне, и они могут быть куда разнообразнее. Это, например, попытка взлома системы через найденную уязвимость: злоумышленник проникает в сеть, чтобы украсть или повредить информацию. Или DDoS-атака, когда на веб-адрес приходит огромное количество запросов с разных адресов, и сервер не выдерживает, а сайт перестает работать.

Сюда же можно отнести деятельность компьютерных вирусов: они способны серьезно навредить работе системы. Действия таких вредоносных программ могут быть очень разнообразными: от рассылки спама от имени взломанного адреса до полной блокировки системы и повреждения файлов.

Еще к внешним угрозам безопасности относятся форс-мажоры и несчастные случаи.

Например, хранилище данных оказалось повреждено в результате аварии или пожара. Такие риски тоже нужно предусмотреть [2].

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

Безопасность информации – состояние защищенности данных, при которых обеспечены их доступность, конфиденциальность и целостность.

Информационная безопасность организации должна включать следующие мероприятия:

1. Анализ потенциальных внешних и внутренних угроз.
2. Оценка уязвимости и защиты информации.
3. Создание дорожной карты мер предотвращения угроз.
4. Выполнение задач по ликвидации угроз.

Главная роль обеспечения защиты данных на предприятии – это создать необходимые условия для бесперебойной работы информационной системы и предотвращение возможных атак на нее [1].

Защита информации включает полный комплекс мер по обеспечению целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права.

Целостность – понятие, определяющее сохранность качества информации и ее свойств.

Конфиденциальность предполагает обеспечение секретности данных и доступа к определенной информации отдельным пользователям.

Доступность – качество информации, определяющее ее быстрое и точное нахождение конкретными пользователями [2].

Безопасность информации на предприятии основывается на пяти принципах:

1. Принцип системности. Защитные меры организации должны быть направлены на предотвращение информационной атаки как со стороны внешних нарушителей, так и со стороны внутренних. При этом необходимо учитывать каналы закрытого доступа, применяемые средства защиты. Применение средств защиты должно совпадать с вероятными видами угроз и функционировать как комплексная система защиты, технически дополняя друг друга. Комплексные методы и средства обеспечения информационной безопасности организации являются сложной системой взаимосвязанных между собой процессов.

2. Принцип многоуровневой защиты направлен на создание рубежей защиты информационной системы, состоящих из последовательно расположенных зон безопасности, главная из которых будет находиться внутри всей системы.

3. Принцип прочности. Правила обеспечения информационной безопасности в организации должны охватывать весь спектр зон безопасности. Все они должны быть иметь одинаковую степень надежной защиты с определением возможной угрозы.

4. Принцип благоразумности представляет собой разумное применение защитных мер с необходимой степенью безопасности. Данный принцип обусловлен целесообразностью огромных материальных затрат и дальнейшей рациональности их использования. Себестоимость мер защиты не должна быть больше размера вероятного ущерба, а также расходы на работоспособность и обслуживание защитной системы.

5. Принцип бесперебойности. Функционирование информационной безопасности должна быть непрерывной и бесперебойной [3, с. 35-38].

С целью минимизации угроз информационной безопасности организации используются следующие методы:

1. Препятствие. Метод представляет собой использование физической силы с целью защиты информации от преступных действий злоумышленников с помощью запрета на доступ к информационным носителям и аппаратуре.

2. Управление доступом – метод, который основан на использовании регулирующих ресурсов автоматизированной системы, предотвращающих доступ к информационным носителям. Управление доступом осуществляется с помощью таких функций, как:

- идентификация личности пользователя, работающего персонала и систем информационных ресурсов такими мерами, как присвоение каждому пользователю и объекту личного идентификатора;

- аутентификация, которая устанавливает принадлежность субъекта или объекта к заявленному им идентификатору;
- проверка соответствия полномочий, которая заключается в установлении точного времени суток, дня недели и ресурсов для проведения запланированных регламентом процедур;
- доступ для проведения работ, установленных регламентом и создание необходимых условий для их проведения;
- регистрация в виде письменного протоколирования обращений к доступу защитных ресурсов;
- реагирование на попытку несанкционированных действий в виде шумовой сигнализации, отключения, отказа в запросе и в задержке работ.

3. Маскировка – метод криптографического закрытия, защищающий доступ к информации в автоматизированной системе.

4. Регламентация – метод информационной защиты, при котором доступ к хранению и передаче данных при несанкционированном запросе сводится к минимуму.

5. Принуждение – это метод, который вынуждает пользователей при доступе к закрытой информации соблюдать определенные правила. Нарушение установленного протокола приводит к штрафным санкциям, административной и уголовной ответственности.

6. Побуждение – метод, который основан на этических и моральных нормах, накладывающих запрет на использование запрещенной информации, и побуждает соблюдать установленные правила [2].

Все перечисленные методы защиты основаны на следующих средствах:

1. Система физической защиты (СФЗ). Применяется в качестве внешнего контроля за месторасположением объекта и защиты информационной системы в виде специальных устройств. Рассмотрим основные элементы СФЗ (табл.).

Таблица

№	Элемент СФЗ	Характеристика
1	Глубоко эшелонированная защита	Направлена на создание многоуровневой системы преград для внешнего нарушителя
2	Система видеонаблюдения	С помощью данной системы распознается нарушитель
3	Система контроля доступа к объектам	Автоматизированная информационная система, позволяющая определить лицо, имеющее доступ к объектам

Так, основными элементами СФЗ являются защита в виде автоматизированной системы ограждения, систем видеонаблюдения и система контроля доступа к объектам. Все эти элементы СФЗ должны находиться на постоянном контроле согласно утвержденному порядку в организации.

2. Аппаратные средства защиты представлены электронными и автоматизированными механическим устройствам. Они встроены в блоки автоматизированной информационной системы, представляющие собой самостоятельные устройства, соединенные с данными блоками.

Основная их функция – это обеспечение внутренней защиты соединительных элементов и систем в вычислительной технике – периферийного оборудования, терминалов, линий связи, процессоров и других устройств.

Обеспечение безопасности информации с помощью аппаратных средств включает:

1. Обеспечение запрета неавторизированного доступа удаленных пользователей и АИС (автоматизированная информационная система);

2. Обеспечение надежной защиты файловых систем архивов и баз данных при отключениях или некорректной работе АИС;

3. Обеспечение защиты программ и приложений.

Вышеперечисленные задачи обеспечения безопасности информации обеспечивают аппаратные средства и технологии контроля доступа (идентификация, регистрация, определение полномочий пользователя).

Обеспечение безопасности особо важной информации может осуществляться с использованием уникальных носителей с особыми свойствами, которые предотвращают считывание данных [3, с. 35-38].

Программные средства защиты входят в состав ПО (программного обеспечения), АИС или являются элементами аппаратных систем защиты. Такие средства относятся к наиболее популярным инструментам защиты осуществляют, обеспечивают безопасность информации

путем реализации логических и интеллектуальных защитных функций и. Это объясняется их доступной ценой, универсальностью, простотой внедрения и возможностью доработки под конкретную организацию или отдельного пользователя. В то же время, обеспечение безопасности информации с помощью ПО является наиболее уязвимым местом АИС организаций.

Таким образом, используя максимально различные способы защиты, служба информационной безопасности создает такую систему информационной безопасности, которая позволяет сохранить информационные данные, снизить до минимума риски несанкционированного доступа к различному рода сведениям, имеющим важное значение для функционирования организации [3, с. 35-38].

Заключение

Меры по обеспечению информационной безопасности на предприятии должны разрабатываться и реализовываться постоянно, независимо от роли IT-инфраструктуры в производственных процессах.

К решению этого вопроса необходимо подходить комплексно и с привлечением сторонних специалистов. Только такой подход позволит предотвратить утечку данных, а не бороться с ее последствиями.

Литература

1. Храмогин П.А. Принципы информационной безопасности, 2014.

2. Грошева Е.К., Невмержицкий П.И. Информационная безопасность: современные реалии, 2017.

3. Осадчий В.В. Основы инвестирования. Правила для начинающих инвесторов / В.В. Осадчий // Управленческий учет. – 2020. – № 4. – С. 35-38.

4. Осадчий В.В. Сложные проценты в инвестировании как восьмое чудо света / В.В. Осадчий // Актуальные вопросы современной экономики. – 2021. – № 3. – С. 100-105. – DOI 10.34755/ИРОК.2021.62.75.087.

GERASIMOV Andrei Sergeevich
general manager, Digital Group LLC, Russia, Moscow

SAFETY IN THE ORGANIZATION

Abstract. *Any public or private enterprise is obliged to reliably and effectively ensure information security. This is very important, because technology is constantly developing, and the scope of application of computers and other equipment is expanding. Information security goals are formed based on the tasks facing the cybersecurity system of an individual company. The more important the data, the more it needs to be protected. Constantly developing information security tools monitor any changes in the system code and attempts of unauthorized entry into the information storage. If you devote little time and money to cybersecurity, catastrophic consequences can occur in the form of loss of important information, infection with malicious codes, unauthorized access of unauthorized persons to a data bank, etc. The main task of information security is to limit such situations as much as possible and provide for all potential dangers. The higher the reliability of the system, the lower the likelihood of hacking.*

Keywords: *information security (IS) in an organization, data protection, physical protection system, hardware protection, software protection tools.*

ГЕРАСИМОВ Андрей Сергеевич
генеральный директор, ООО «Диджитал Групп»,
Россия, г. Москва

ОБЛАЧНЫЕ СЕРВИСЫ В СИСТЕМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

Аннотация. *Системы поддержки принятия решений (СППР) – компьютерные автоматизированные системы, целью которых является помощь людям, принимающим решение в сложных условиях, для полного и объективного анализа предметной деятельности. СППР возникли в результате слияния управленческих информационных систем и систем управления базами данных. Знание принципов построения современных систем поддержки принятия решений (СППР), основу технологий хранилищ данных, оперативного анализа для аналитической поддержки процессов принятия решений является необходимым знанием в подготовке IT-специалистов.*

Ключевые слова: *облачные сервисы, система поддержки принятия решений (СППР), база данных, интерактивные системы, облако.*

Основная часть

Система поддержки принятия решений – это компьютерная система, которая путем сбора и анализа большого количества информации может влиять на процесс принятия решений организационного плана в бизнесе и предпринимательстве. Интерактивные системы позволяют руководителям получить полезную информацию из первоисточников, проанализировать ее, а также выявить существующие бизнес-модели для решения определенных задач [3].

СППР позволяет спрогнозировать доход организации при гипотетическом внедрении новой технологии, проследить за всеми доступными информационными активами и получить сравнительные значения объемов продаж, а также рассмотреть все возможные альтернативные решения.

Система поддержки принятия решений – комплекс математических и эвристических методов и моделей, которые объединены общей методикой формирования альтернатив управленческих решений в организационных системах, определения последствий реализации каждой альтернативы и обоснования выбора наиболее приемлемого управленческого решения [3].

Поддержка принятия решений и заключается в помощи лицу, принимающему решение (ЛПР), в процессе принятия решений. Она включает:

- помощь ЛПР при анализе объективной составляющей, то есть в понимании и оценке сложившейся ситуации, и ограничений, накладываемых внешней средой;
- выявление предпочтений ЛПР, то есть выявление и ранжирование приоритетов, учет неопределенности в оценках ЛПР и формирование его предпочтений;
- генерацию возможных решений, то есть формирование списка альтернатив;
- оценку возможных альтернатив, исходя из предпочтений ЛПР, и ограничений, накладываемых внешней средой;
- анализ последствий принимаемых решений;
- выбор лучшего с точки зрения ЛПР варианта.

СППР в большинстве случаев служит как интерактивная автоматизированная система, она же помогает ЛПР использовать данные и модели для идентификации и решения задач и принятия решений. Система должна обладать возможностью работать с интерактивными запросами с достаточно простым для изучения языком [2, с. 100-105].

СППР обладает следующими четырьмя основными характеристиками:

1. Использует и данные, и модели;
2. Помогает менеджерам в принятии решений для слабоструктурированных и неструктурированных задач;
3. Поддерживает, а не заменяет выработку решений менеджерами;
4. Повышает эффективность решений.

Идеальная СППР:

1. Оперирует со слабоструктурированными решениями;

2. Предназначена для ЛПР различного уровня;

3. Может быть адаптирована для группового и индивидуального использования;

4. Поддерживает как взаимозависимые, так и последовательные решения;

5. Поддерживает три фазы процесса решения: интеллектуальную, проектирование и выбор;

6. Поддерживает разнообразные стили и методы решения, что может быть полезно при решении задачи группой ЛПР;

7. Является гибкой и адаптируется к изменениям как организации, так и ее окружения;

8. Проста в использовании и модификации;

9. Улучшает процесс принятия решений;

10. Позволяет человеку управлять процессом принятия решений с помощью компьютера;

11. Поддерживает эволюционное использование и легко адаптируется к изменяющимся требованиям;

12. Может быть легко построена, если сформулирована логика конструкции СППР;

13. Поддерживает моделирование;

14. Позволяет использовать знания [2, с. 100-105].

Компьютерная поддержка процесса принятия решений так или иначе основана на формализации методов получения рекомендаций, даваемых ЛПР, и алгоритмизации самого процесса выработки решения.

К тому же, формализация методов генерации решений, их оценка и согласование являются чрезвычайно сложной задачей. Эта задача стала интенсивно решаться с возникновением вычислительной техники.

Все больше предприятий рассматривают возможность перехода к облачным технологиям, которые имеют огромный потенциал для существенного повышения эффективности без ущерба для производительности. Популярность облачных ИТ доказывается тем, что по результатам исследований аналитических компаний Forrester Research, IDC, российской ассоциации электронных коммуникаций (РАЭК) мировой рынок облачных услуг вырос на 90 % в 2023 г. [1, с. 35-38].

Облачные вычисления – быстро развивающаяся область IT. Термин «облачные вычисления» появился чуть более пяти лет назад. На рынке информационных технологий уже предлагаются комплексные решения, которые позволяют предоставлять облачные сервисы различным категориям потребителей: финансовому сектору, промышленности, торговле, сфере услуг, сектору телекоммуникаций и, конечно, науке и образованию.

«Облако» (cloud computing) обозначает сложную инфраструктуру с большим количеством технических деталей, спрятанных в «облаках». Облачные системы связаны как с рисками, характерными исключительно для таких систем, так и с инструментами, которые могут быть применены для управления ими. Используя облачную структуру, вы делите ее с большим числом людей, при этом у вас в руках очень немного инструментов, делающих возможность контролировать то, как люди будут использовать этот общественный ресурс. Существуют методы, позволяющие сделать систему безопасной изначально, вместо того чтобы полагаться на аттестаты безопасности, которые предлагает поставщик услуг облачных вычислений [1, с. 35-38].

Положительными сторонами использования облачных технологий можно назвать следующие:

- Доступность: доступ к информации, хранящейся на облаке, может получить каждый, кто имеет компьютер, планшет, любое мобильное устройство, подключенное к сети интернет. Из этого вытекает следующее преимущество.
- Мобильность: у пользователя нет постоянной привязанности к одному рабочему месту. Из любой точки мира менеджеры могут получать отчетность, а руководители – следить за производством.
- Экономичность: одним из важных преимуществ называют уменьшенную затратность. Пользователю не надо покупать дорогостоящие, большие по вычислительной мощности компьютеры и ПО, а также он освобождается от необходимости нанимать специалиста по обслуживанию локальных IT-технологий.
- Арендность: пользователь получает необходимый пакет услуг только в тот момент, когда он ему нужен, и платит, собственно, только за количество приобретенных функций.
- Гибкость: все необходимые ресурсы предоставляются провайдером автоматически.
- Высокая технологичность: большие вычислительные мощности, которые предоставляются в распоряжение пользователя, которые можно использовать для хранения, анализа и обработки данных.

• Надежность: некоторые эксперты утверждают, что надежность, которую обеспечивают современные облачные вычисления, гораздо выше, чем надежность локальных ресурсов, аргументируя это тем, что мало предприятий могут себе позволить приобрести и содержать полноценный ЦОД [2, с. 100-105].

Обобщая структуру разрабатываемой системы поддержки принятия решений, можно представить из следующих базовых модулей:

1. Сбор данных. В данном модуле происходит сбор статистических данных, а также данных, предоставленных пользователем в ходе взаимодействия с программным интерфейсом разрабатываемой системы.

2. Хранилище данных. Хранение данных, собранных в первом модуле, производится в облачной базе данных.

3. Аналитическая система. В данном модуле происходит обработка данных согласно предложенной экономико-математической модели.

4. Система поддержки принятия решений (СППР). Модуль, обеспечивающий взаимодействие лица, принимающего решение, с данными, обработанными системой.

Хранение данных в разрабатываемой СППР организовано в виде база данных с использованием облачных технологий, применение которой обусловлено необходимостью накопления больших данных для принятия решений.

Технология облачного хранения данных использует модель онлайн-хранилища, в котором все данные хранятся размещенных в сети. Данные хранятся представляющем собой абстрактный виртуальный сервер. Физически эти серверы могут быть расположены территориально удалённо друг от друга географически. С позиции организации, для него наглядно, что все действия осуществляются в одном месте – «облаке» [3].

Заключение

Развитие науки и техники значительно ускорило появление новых достижений в сфере ИТ во всех сферах социально-экономической жизни общества. Применение ИТ позволяет справиться с огромным объемом обрабатываемой информации и способствует сокращению сроков ее обработки и поддержки принятия решений. Внедрение проекта в области ИТ «облака» представляет собой как сбор и хранилища базы данных, являющийся более масштабным, и как этап для поддержки принятия решения.

Литература

1. Осадчий В.В. Основы инвестирования. Правила для начинающих инвесторов / В.В. Осадчий // Управленческий учет. – 2020. – № 4. – С. 35-38.

2. Осадчий В.В. Сложные проценты в инвестировании как восьмое чудо света / В.В. Осадчий // Актуальные вопросы современной экономики. – 2021. – № 3. – С. 100-105. – DOI 10.34755/ИРОК.2021.62.75.087.

3. Гребнев Е. Облачные сервисы. Взгляд из России, 2021.

GERASIMOV Andrei Sergeevich
general manager, Digital Group LLC, Russia, Moscow

CLOUD SERVICES IN SUPPORT SYSTEMS DECISION MAKING

Abstract. *Decision support systems (DSS) are computer automated systems, the purpose of which is to help people making decisions in difficult conditions for a complete and objective analysis of subject activity. DSS emerged from the merger of management information systems and database management systems. Knowledge of the principles of building modern decision support systems (DSS), the basis of data warehouse technologies, operational analysis for analytical support of decision-making processes is necessary knowledge in the training of IT specialists.*

Keywords: *cloud services, decision support system (DSS), database, interactive systems, cloud.*

МОРОЗКИН Степан Алексеевич
магистрант,
Московский государственный технологический университет «Станкин»,
Россия, г. Москва

«УМНЫЙ» СТЕЛЛАЖ «SMARTBOX» НА БАЗЕ ARDUINO ДЛЯ ХРАНЕНИЯ ИНСТРУМЕНТОВ

Аннотация. *Рассматриваются вопросы, связанные с проектированием вспомогательного оборудования (на примере «умного» стеллажа для инструментов с голосовым управлением), предназначенного для оснащения машиностроительных предприятий, нацеленных на переход на концепцию «Индустрия 4.0». Приводится описание таких этапов проектирования, как создание идеи, разработка электронной схемы, конструирование изделия в САПР, производство и тестирование опытного образца.*

Ключевые слова: *«smart» производство, «Индустрия 4.0», Arduino.*

Переход производственных систем на новый уровень в рамках концепции «Индустрия 4.0» невозможен без тотальной цифровизации всех информационных потоков, включая и голосовое (вербальное) общение. В таком производстве все оборудование (основное, вспомогательное, производственное, непроизводственное), компьютеры, нейросети, облачные сервисы, а также люди будут объединены в некую единую «умную» производственную систему, работающую в режиме 24/7 [1, с. 6-8].

Но если станки и компьютеры могут «говорить» на едином языке цифровых сигналов, то для интеграции человека в эту систему необходимо предоставить ему удобный интерфейс. Обычно таким связующим звеном выступал компьютер или терминал, с которого работник мог вводить запросы, получать или вносить информацию. Однако на современном этапе развития искусственного интеллекта уже можно предложить более совершенный подход.

Рассмотрим ситуацию на конкретном примере.

Производственному рабочему необходимо быстро найти в инструментальной раздаточной кладовой нужный инструмент (торцевую фрезу, центровочное сверло, отрезной резец и т. п.). Инструменты обычно хранятся в универсальных и специализированных стеллажах, шкафах, кассетах, стендах (рис. 1). Рабочий может обратиться к складской базе данных инструментов, найти нужный стеллаж по надписям или кодам, или обратиться к работнику кладовой.

Для нахождения информации в сети интернет с использованием компьютеров и смартфонов уже давно применяется голосовой поиск. Эту идею можно применить и для поиска нужного инструмента на складе. Однако для этого потребуется использование «умных» стеллажей или «умной» системы навигации по складу.

Несмотря на то, что возможности применения концепции голосового поиска и голосового управления в производстве значительно шире данной задачи, рассмотрим вопросы, связанные с проектированием подобных систем в условиях западных санкций и импортозамещения.

Рис. 1. Типы стеллажей в инструментально-раздаточной кладовой

Для реализации идеи «умного» стеллажа потребуется микроконтроллер с интерфейсом беспроводной связи, а также система индикации для указания (подсвечивания) расположения инструмента на стеллаже.

Для распознавания речи можно воспользоваться готовыми решениями [2], например, от отечественной компании Яндекс, а электронную часть «умного» стеллажа можно выполнить на базе микроконтроллера семейства Arduino, производимого по всему миру, в том числе, в России. Таким образом, будет достигнута полная независимость от западных технологий и санкций.

Схему работу системы можно описать следующим образом (рис. 2). Работник произносит название инструмента, которое распознается в приложении для смартфона и передается по беспроводному каналу связи в микроконтроллер уже в виде структурированного текстового (символьного) сообщения. Контроллер сравнивает полученное название с записями базы данных и подсвечивает необходимый ящик или позицию стеллажа с помощью светодиодов.

Электронная схема устройства при таком подходе окажется очень простой (рис. 3) и дешевой, что позволит легко внедрить «умную начинку» и в уже действующую небольшую складскую систему.

Рис. 2. Схема работы голосового управления

Так как плата ArduinoUNO [3, с. 25-29]имеет всего 14 цифровых выходов, два из которых задействованы для модуля Bluetooth-связи HC-05, то максимальное управляемых для подсветки или сигнализации светодиодов равно 12. Применение четырех регистров сдвига 74HC595 позволит увеличить их число до 24, что вполне достаточно для одной-двух секций большого стеллажа инструментальной кладовой. Применение же платы ArduinoMegac 54 цифровыми выходами [2] и 17 регистрами сдвига 74HC595 позволит адресно охватить до 136 ячеек (ящиков) большого инструментального стеллажа.

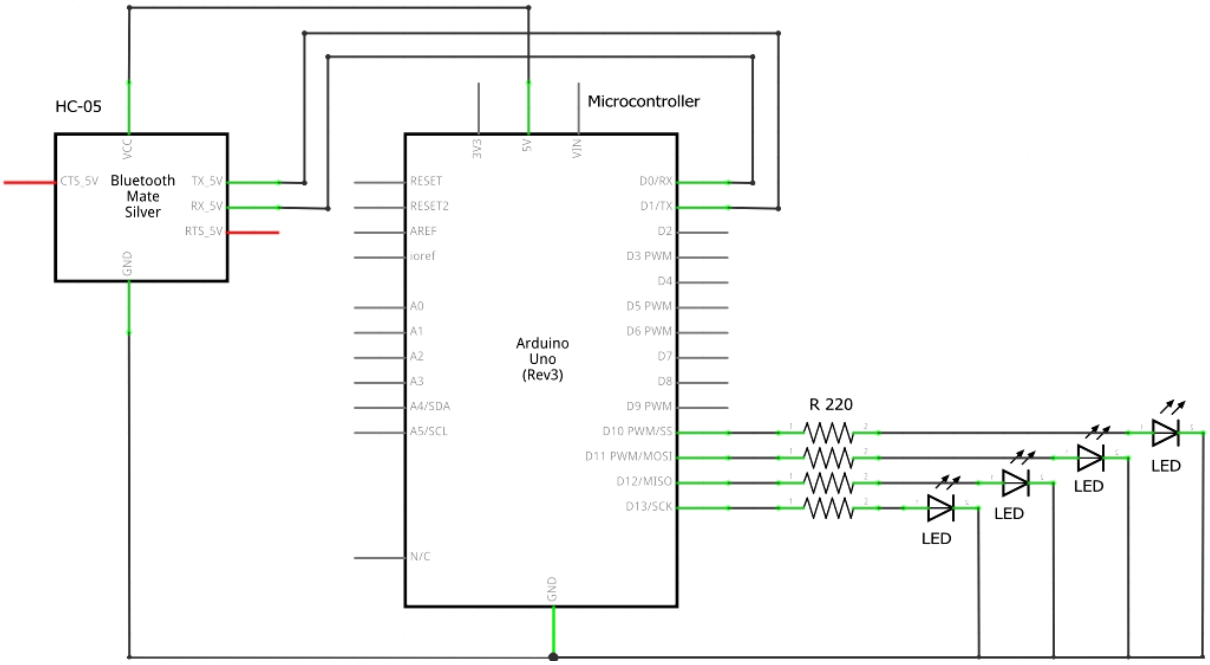


Рис. 3. Электрическая схема «умного» стеллажа

На рисунке 4 показана цифровая модель опытного образца такого «умного» стеллажа – SMARTBOX, разработанная в отечественной конструкторской САПР – КОМПАС 3D.

Стеллаж-прототип, изготовлен из плит ДСП и МДФ, имеет всего 4 ящика для хранения инструментов средних размеров (фрез, сверл, резцов, гаечных ключей и т. п.). Микропроцессорный блок управления, реализованный на плате ArduinoUNO, размещен в задней части стеллажа, а подсветка ящиков реализована с помощью светодиодов различного цвета, расположенных над ящиками. Связь Arduino со смартфоном осуществляется по каналу Bluetooth через модуль HC-05.

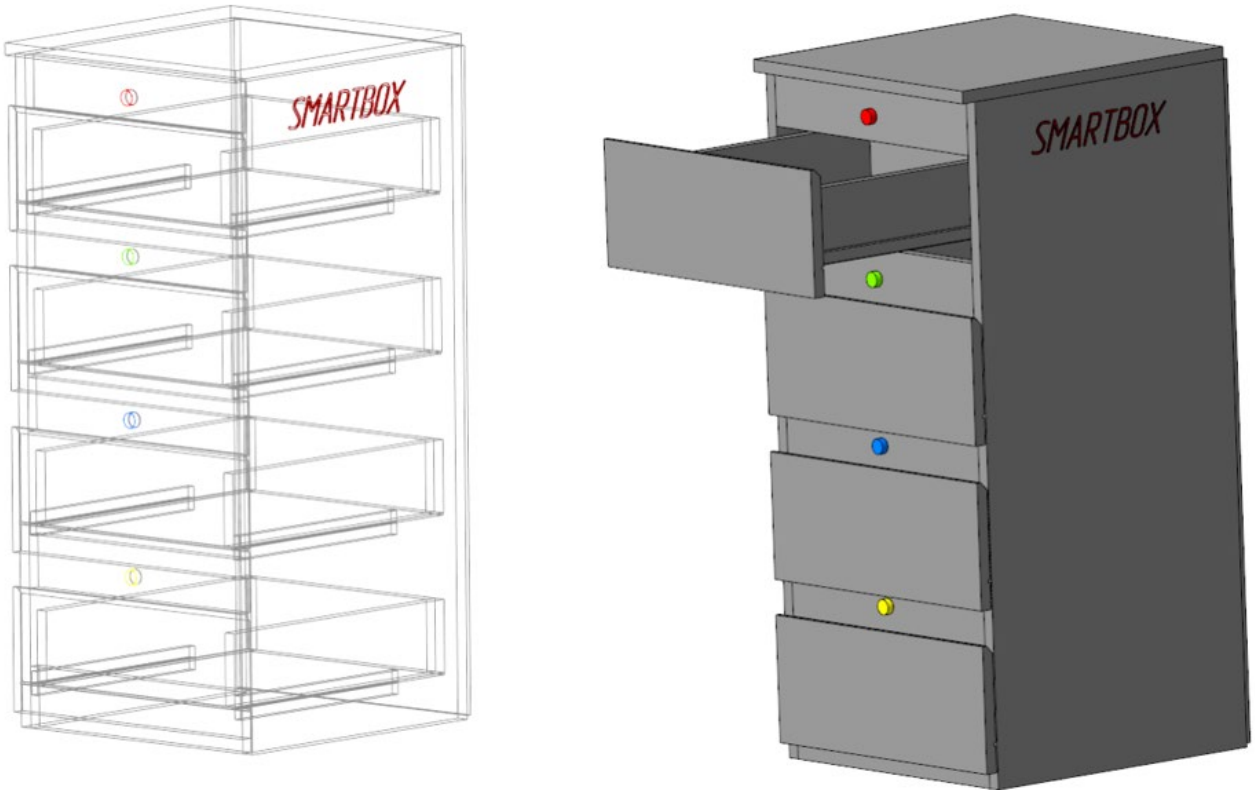


Рис. 4. Трехмерная модель «умного» стеллажа SMARTBOX

Таким образом, можно сделать вывод о том, что разработка современного вспомогательного оборудования для производственных предприятий, переходящих на концепцию «Индустрия 4.0» вполне является посильной задачей, решения которой можно добиться, опираясь только на отечественные технологии (аппаратные, производственные, программные) и технологии с открытым доступом [4].

Перспективы же интеграции голосового общения человека, компьютера и производственной системы многочисленны, и помимо рассмотренного в статье голосового поиска предметов (инструментов), могут включать управление «умным» оборудованием, элементами системы контроля и безопасности предприятия и пр.

Литература

1. Петрушенко, А.А. Речевые технологии – следующий уровень сервиса / А.А. Петрушенко, Р.В. Петрушенко. – Текст: непосредственный // Технические науки в России и за рубежом: материалы V Междунар. науч. конф. (г. Москва, январь 2016 г.). – Москва: Буки-Веди, 2016. – С. 6-8. – URL: https://moluch.ru/conf/tech/archive/164.

2. С. Монк. Программируем Arduino. Профессиональная работа со скетчами. – СПб.: Питер, 2017. ISBN 978-5-496-02385-6.

3. Махов А.А. Повышение качества учебных и любительских проектов на базе Arduino с помощью технологий трехмерного моделирования. Вестник МГТУСТАНКИН. 2021. № 4 (59). С. 25-29.

4. https://trends.rbc.ru/trends/industry/5e740c5b9a79470c22dd13e7 – Что такое индустрия 4.0 и что нужно о ней знать | РБК Тренды (rbc.ru).

MOROZKIN Stepan Alekseevich
Graduate student,
Moscow State Technological University "Stankin",
Russia, Moscow

"SMART" ARDUINO-BASED SMARTBOX CABINET FOR STORING TOOLS

Abstract. *Some questions concerning development of «smart» equipment with voice control for storing tools, which can be used in industrial company, working accordingly the conception of «Industry 4.0» is discussed in this article. The description of design stages as the creation of an idea, the development of an electronic circuit, the designing of the device in CAD, the producing and testing of the prototype is given.*

Keywords: *«smart» manufacturing, «Industry 4.0», Arduino.*

ПРОНИН Алексей Сергеевич
студент, Нижегородский государственный технический университет им. Р. Е. Алексеева, Россия, г. Нижний Новгород

Научный руководитель – доцент кафедры информационной безопасности вычислительных систем и сетей Нижегородского государственного технического университета им. Р. Е. Алексеева, кандидат технических наук Ляхманов Дмитрий Александрович

СРАВНЕНИЕ И ОЦЕНКА МЕТОДОВ АВТОРИЗАЦИИ И АУТЕНТИФИКАЦИИ В ПРИЛОЖЕНИЯХ PYTHON С ПОМОЩЬЮ МЕТОДА АНАЛИТИЧЕСКОЙ ИЕРАРХИИ

Аннотация. *В данной работе проводится исследование методов авторизации и аутентификации в приложениях Python. С помощью метода аналитической иерархии выполнено сравнение методов по выбранным критериям. Результаты исследования могут быть полезны для выбора методов авторизации и аутентификации при разработке приложений на Python.*

Ключевые слова: *авторизация и аутентификация, информационная безопасность, Python, метод аналитической иерархии.*

Вопрос безопасности информации и личных данных поднимается во всех сферах деятельности, в то время как авторизация и аутентификация являются одними из основных процессов обеспечения защиты и сохранности данных [1, с.172]. Разработка приложений на Python включает в себя значительное внимание к обеспечению безопасности пользовательских данных, осуществляемое с помощью эффективных методов авторизации и аутентификации.

Целью данной статьи является сравнение различных методик авторизации и аутентификации в приложениях Python, с использованием метода аналитической иерархии. Основные задачи исследования включают анализ критериев сравнения различных методов, оценку их эффективности и разработку рекомендаций для разработчиков в области безопасности данных.

Для решения поставленной задачи и выбора оптимального метода, будет применен метод анализа иерархий. Метод аналитической иерархии является одним из способов решения сложных задач с большим количеством элементов, условий, их взаимосвязей и других критериев. Этот метод - математическая формализация всех критериев и условий поставленной задачи [2, с. 63].

Каждый метод авторизации и аутентификации будет оценен по 10-балльной шкале для каждого критерия. Высшая оценка - 10, будет означать абсолютное положительное преимущество данного метода перед альтернативами, которые получили оценку ниже. Этот подход позволит нам систематически проанализировать и оценить каждый метод с учетом его сильных и слабых сторон, что позволит выделить наиболее эффективные и безопасные методы авторизации и аутентификации для приложений на Python.

В данной работе взяты следующие методы авторизации и аутентификации:

– Basic: отправка пары логин/пароль;
– Token-based: использование токенов как идентификаторов;
– Social: вход с помощью социальных сетей;
– 2FA: двухфакторная аутентификация;
– Biometric: использование биометрических данных.

Для сравнения указанных выше альтернатив используются следующие критерии:

– Уровень безопасности: оценка таких параметров, как возможность взлома злоумышленником и защиту от атак посредника, проанализировать слабые точки метода;
– Простота реализации: оценка легкости внедрения метода, его гибкости, адаптивности, интеграции с другими методами;
– Поддержка сообщества: наличие подробной документации и информационных

ресурсов с хорошо структурированными руководствами и часто задаваемыми вопросами;

– Использование ресурсов: анализ затрат таких ресурсов, как: память, время и другие ресурсы, необходимые для функционирования метода;

– Долгосрочная перспектива: степень популярности метода среди разработчиков и пользователей, востребованность на рынке, уровень доверия со стороны сообщества, перспектива развития метода.

По итогу оценки выбранных методов авторизации и аутентификации по необходимым критериям получим следующую таблицу:

Таблица 1

Основные показатели существенных признаков альтернатив

	от 0 до 10, где 10 - лучший результат				
	Уровень безопасности	**Простота реализации**	**Поддержка сообщества**	**Использование ресурсов**	**Долгосрочная перспектива**
Basic A1	3	9	5	9	3
Token-based A2	7	7	8	8	8
Social A3	2	6	4	6	6
2F A4	9	7	9	7	9
Biometric A5	8	4	6	4	10

Определим следующие количественные значения для уровней важности:

Таблица 2

Уровни важности критериев

Уровень важности	Количественное значение
Равная важность	1
Умеренное превосходство	3
Существенное или сильное превосходство	5
Значительное (большое) превосходство	7
Очень большое превосходство	9

И заполним шкалу относительной важности для выбранных критериев:

Таблица 3

Шкала относительной важности критериев

Критерии	**Уровень безопасности**	**Простота реализации**	**Поддержка сообщества**	**Использование ресурсов**	**Долгосрочная перспектива**	**Среднее геометрическое**	**Вес критерия**
Уровень безопасности	1	9	7	3	5	3,936283427	0,510038725
Простота реализации	0,111111111	1	0,333333333	0,142857143	0,2	0,254046747	0,032917772
Поддержка сообщества	0,142857143	3	1	0,2	0,333333333	0,49111861	0,063636045
Использование ресурсов	0,333333333	7	5	1	3	2,036168005	0,263833779
Долгосрочная перспектива	0,2	5	3	0,333333333	1	1	0,129573679
					СУММА:	7,717616789	1

Исходя из данных таблицы 1 проведем сравнение альтернатив по каждому критерию с целью получения веса альтернатив. После расчета весов альтернатив получим следующую общую таблицу:

Таблица 4

Веса альтернатив

	Уровень безопасности	Простота реализации	Поддержка сообщества	Использование ресурсов	Долгосрочная перспектива
Basic A1	0,046678424	0,522412461	0,067932388	0,492329474	0,029685425
Token-based A2	0,191954215	0,182537998	0,275089235	0,242188875	0,185030249
Social A3	0,032620149	0,080286777	0,03388191	0,075663484	0,068867945
2F A4	0,437799029	0,182537998	0,52070872	0,158627083	0,284350094
Biometric A5	0,290948183	0,032224766	0,102387747	0,031191085	0,432066286

Получим значения для каждой альтернативы по формуле $V_j = \sum_{j=1}^{k} w_i V_{ji}$:

Таблица 5

Значения альтернатив

Альтернатива	Значение
Basic A1	0,179067002
Token-based A2	0,209291074
Social A3	0,050322568
2F A4	0,341134517
Biometric A5	0,220184839

Важно, чтобы сумма значения равнялась 1. Так мы проверим согласованность решения. Отсортируем по убыванию и получим следующий результат:

Лучшей альтернативой является альтернатива № 4 – 2FA (двухфакторая аутентификация).

Таким образом, выбрав необходимые критерии при разработке системы авторизации и аутентификации и определив их количественные значения для уровней важности, а после оценив показатели существенных признаков альтернатив, с помощью метода аналитической иерархии можно получить количественную оценку каждой альтернативы по выбранным критериям для выбора внедряемого метода. Этот способ может не только помочь в выборе метода авторизации и аутентификации при разработке приложения, но также наглядно отразить сильные и слабые стороны каждых методов в сравнении друг с другом.

Литература

1. Костиков Ю. А., Романенков А. М. Методы организации безопасных механизмов авторизации и аутентификации // Сборник научных трудов кафедры прикладной математики и программирования по итогам работы постоянно действующего семинара «Теория систем», 2022. 366 с.

2. Васильев, А. А. Метод аналитической иерархии, как один из главных методов принятия решения по усовершенствованию маршрутов // Наука в современном обществе: закономерности и тенденции развития, 2022. 296 с.

PRONIN Alexey Sergeevich
Student of the Chair of Informatics and Control Systems,
Nizhny Novgorod State Technical University n.a. R.E. Alekseev,
Russia, Nizhny Novgorod

Scientific Advisor – Associate Professor of the Chair of Information Security of Computer Systems and Networks, Nizhny Novgorod State Technical University n.a. R.E. Alekseev, Cand. Sc. (Technology) Lyakhmanov Dmitry Alexandrovich

COMPARISON AND EVALUATION OF AUTHORIZATION AND AUTHENTICATION METHODS IN PYTHON APPLICATIONS USING ANALYTIC HIERARCHY METHOD

Abstract. *This paper investigates authorization and authentication methods in Python applications. Using the analytic hierarchy method, the methods are compared according to the selected criteria. The results of the study can be useful for selecting authorization and authentication methods for Python application development.*

Keywords: *authorization and authentication, information security, Python, analytic hierarchy method.*

ТОРОБЦЕВ Игорь Александрович
магистрант,
Донбасский государственный технический университет, г. Алчевск

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МОНИТОРИНГА ФИНАНСОВО-ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Аннотация. *В данной статье рассматривается важность обеспечения своевременной, достоверной информацией и принятия оптимальных управленческих решений для обеспечения жизне- и конкурентоспособности предприятий. Основное внимание уделяется аудиту результатов финансово-хозяйственной деятельности и мониторингу результатов в динамике. Также обсуждается значимость управленческого учета и анализа для эффективного управления предприятиями.*

Ключевые слова: *информация, управленческие решения, финансово-хозяйственная деятельность, аудит, мониторинг, управленческий учет, анализ.*

В наше время обеспечение жизне- и конкурентоспособности предприятия возможно при условии обеспечения своевременной и достоверной информацией, обеспечивающей принятие оптимальных управленческих решений, обеспечивающих устойчивое текущее и будущее функционирование предприятия [1, с. 44-50].

Эффективность управления структурами предприятия обеспечивается наличием у руководителей необходимой информации и умением ее использовать. В настоящее время наибольшее распространение получил аудит результатов финансово-хозяйственной деятельности, представляющий собой статическую оценку. Однако больший интерес для практики управления представляет оценка результатов финансово-хозяйственной деятельности в динамике, а именно ее мониторинг. Руководитель любого предприятия понимает, что эффективность и успех его организации напрямую зависит от результатов его наблюдений и управленческих решений. В современных условиях руководитель должен периодически получать самые важные сведения по всем подразделениям и отделам, прикладывая при этом минимальное количество усилий [2, с. 9-15].

Все организации ведут бухгалтерский и налоговый учет, которые осуществляется с определенной периодичностью, определяющейся законодательством и внутренними нормативами. Однако ведение управленческого учета не является обязательным. В то же время, организация управленческого учета и анализа позволяет оперативно реагировать на отклонения, возникающие при реализации ФХД.

Анализ финансовой и управленческой информации обеспечивает выявление состояния ФХД, определяющее текущую ситуацию и актуальные проблемы предприятия. Такая информация должна быть как оперативной, так и аналитической. Под управленческой информацией понимается совокупность сведений о процессах, протекающих внутри фирмы и ее окружении. Финансовая информация переставлена финансовыми показателями, отражающими финансовые результаты деятельности и финансовое состояние предприятия [3, с. 72-75].

Состояние финансово-хозяйственной деятельности (ФХД) предприятия характеризуют группами показателей [4]:

1. Показатели исходных условий деятельности предприятия.
2. Показатели использования средств производства.
3. Показатели использования предметов труда и трудовых ресурсов.
4. Показатели производства и сбыта продукции.
5. Показатели себестоимости, прибыли и рентабельности.
6. Показатели финансового состояния предприятия.

Все эти показатели характеризуют результат выполнения базовых бизнес-процессов: поставок сырья, материалов и энергии; производства продукции; хранения и доставки

готовой продукции; продажи конечным потребителям.

Подсистему мониторинга ФХД предлагается реализоваться средствами программного обеспечения, которое, как правило, уже есть у предприятия, а именно системы управления базами данных (СУБД). Современные СУБД содержат такие средства, как триггеры – подпрограммы, выполняющиеся при возникновении событий вставки, удаления и обновления записей в таблицах БД. При возникновении событий вставки и обновления проводим анализ возникшего отклонения, сравниваем с индикатором и формируем либо сообщение на электронном табло, либо записываем в журнал. Журнал – это таблица БД, содержащая сведения о выполненных бизнес-процессах, их результатах в натуральной и/или денежной форме, привязанных к бизнес-процессам и индикаторам.

Кроме реакции на отклонения, необходимо реализовать модули в виде процедур СУБД, которые выполняются по расписанию и осуществляют ABC- и XYZ-анализ [5] основных, наиболее значимых показателей, таких как: себестоимость, обеспеченность сырьем, материалами и топливом, текущее финансовое состояние предприятия и др.

Построение программного модуля будет осуществляться на базе клиент-серверной архитектуры. Архитектура клиент-сервер – это архитектура программного комплекса, в которой происходит распределение прикладной программы по двум логически различным компонентам (клиент и сервер), взаимодействующим по схеме «запрос-ответ» и решающим свои определенные задачи. Это дает следующие преимущества [6]:

- масштабируемость;
- безопасность;
- отказоустойчивость;
- независимое изменение уровней;
- эффективность разработки и внедрения;
- повторное использование.

Одна из основных задач, которую должен выполнять будущий программный модуль – расчет показателей финансово-хозяйственной деятельности предприятия. Существует достаточно большое количество таких показателей. Их использование зависит от специфики предприятия и тех задач, которые оно выполняет. В работе будем ориентироваться на специфику промышленного предприятия.

Литература

1. Безрукова Т.А. Анализ финансово-хозяйственной деятельности организации / Т.А. Безрукова, А.Н. Борисов, И.И. Шанин. – Общество: политика, экономика, право. – 2013. – № 1, С. 44-50.

2. Абдукаримов И.Т. Бухгалтерская (финансовая) отчетность как основной источник мониторинга и анализа финансового состояния предприятия / И. Т. Абдукаримов // Социально-экономические явления и процессы 2012. № 10. С. 9-15.

3. Акежев А.А, Золоева З.Б. Алгоритм формирования управленческой информации / А.А Акежев, З.Б Золоева // Экономический вестник Ростовского государственного университета. 2009. Том 7 № 2 (часть 3). С. 72-75.

4. Савицкая Г.В. Анализ хозяйственной деятельности (АХД): Учебник. – М.: НИЦ ИНФРА-М, 2024. – 378 с.

5. Контроллинг: теория и практика: учебник и практикум для вузов / С.В. Осипов [и др.]; под общей редакцией С.В. Осипова. – Москва: Издательство Юрайт, 2023. – 145 с.

6. Карамнова В.М Сравнение типов клиент-серверной архитектуры/ В.М Карамнова // Молодежный научно-технический вестник. – 2016. – 09, сентябрь.

TOROPTSEV Igor Alexandrovich
graduate student,
Donbass State Technical University, Alchevsk

SOFTWARE IMPLEMENTATION OF MONITORING OF FINANCIAL AND ECONOMIC ACTIVITIES OF THE ENTERPRISE

Abstract. *This article discusses the importance of providing timely, reliable information and making optimal management decisions to ensure the viability and competitiveness of enterprises. The main focus is on auditing the results of financial and economic activities and monitoring the results in dynamics. The importance of management accounting and analysis for the effective management of enterprises is also discussed.*

Keywords: *information, management decisions, financial and economic activities, audit, monitoring, management accounting, analysis.*

МЕДИЦИНА, ФАРМАЦИЯ

ОРЛОВА Эльза
мастер перманентного макияжа международного класса,
Консепт Лайн, США, г. Бока-Ратон

ВНЕДРЕНИЕ ПИГМЕНТА: МОЖНО ЛИ ПРЕДСКАЗАТЬ ИЗМЕНЕНИЯ ЦВЕТА?

Аннотация. *В статье подробно обсуждаются вопросы, связанные с внедрением пигмента в кожу в контексте перманентного макияжа и изменения цвета пигмента после процедуры. Описывается влияние различных факторов, включая качество пигмента, состав ингредиентов и внешние условия, на конечный результат процедуры. Основное внимание уделяется химическому составу пигментов, их классификации, а также законодательным и нормативным актам, регулирующим их использование в разных странах. Обсуждается роль производителя пигмента и необходимость понимания состава пигмента мастерами перманентного макияжа для предсказания и минимизации возможных изменений цвета.*

Ключевые слова: *внедрение пигмента, перманентный макияж, изменение цвета пигмента, химический состав пигментов, классификация пигментов, законодательство и нормативы, качество пигментов, производители пигмента, факторы влияния на цвет, анализ состава пигмента.*

Розовато-оранжевый, красно-фиолетовый, серо-коричневый, полупрозрачный красный… Так описывают на форумах изменения цвета пигмента клиенты и сами мастера перманентного макияжа. Фраза «цвет совершенно непредсказуемо изменился через три месяца после микроблейдинга» сведёт на нет всё впечатление от, казалось бы, идеальной работы визажиста. Но так ли неожиданно мутирует пигмент? Можно ли предсказать и избежать серьёзных колористических коллизий?

Успех процедуры зависит, по сути, от трёх факторов: грамотного исполнения, оборудования и качественных пигментов. С первым условием понятно: собственный профессиональный уровень зависит от знаний, полученных от наставников на курсах, опыта и своей мотивации. С инструментом тоже можно определиться. А вот в ситуации с пигментом появляется, скажем так, второй мастер – компания-производитель красителя. Насколько хорошо мы его знаем? Понимаем ли, из чего изготовлен пигмент, что это, собственно, такое, или перечень ингредиентов на упаковке нам ничего не говорит? Какими законодательными актами, нормативами руководствуется бренд? Что значит «качественный» пигмент? Как его состав может влиять на появление аллергии у клиента? Чтобы дать чёткие ответы, я предлагаю немного побыть химиками-технологами и разобраться в технической стороне пигментного вопроса. Отмечу, что с учётом специфики темы далее в статье будут приводиться термины на английском языке.

Дела фабричные и законодательные

Для предметности разговора возьмём реальное описание состава флакона от итальянского производителя: INCI NOMINATION FD&C Inorganic Pigments, FD&C Organic Pigments, Glicerin, Isopropylic Alcohol, Ricin Oil, Aqua/Water, Propilene Glycol, Aloe Barbadensis, Hammamelis Virginiana, Polysorbate 20, Magnesium Aluminium, Silicate. May contain: Methyl Paraben, Propyl Paraben, Phenoxy Ethanol, PVP, C.I.: 77491-77492-77499-77891-77288-77289-77266-77007-12370-15850:1.

Чтобы это расшифровать, нужно сперва понять: то, что мы в работе называем «пигмент», содержит не только «исходный пигмент», но и другие компоненты. В зарубежных публикациях наш флакон с субстанцией (bottle of pigment) может также обозначаться, как чернила для перманентного макияжа (permanent make-up inks). Их производят в Европе (Германия, Италия, Великобритания, Франция, Испания), в Азии (Китай, Тайвань) и в США. По

некоторым оценкам, европейские производители занимают примерно 70–80% мирового рынка, причём речь идёт о немецких и итальянских брендах. Что же касается сырья, то здесь будут преобладать китайские поставщики.

В законодательстве США и Европейского союза используются две основных дефиниции – «перманентный макияж» (PMU) и «колорант» (colorant). В косметической индустрии к колоранту относят различные типы пигмента – lake/lakes или lake pigment (озеро пигмент или озёрный пигмент), dye/dyes (краситель), pigments (пигмент). При достаточно вольном переводе на русский язык все термины можно интерпретировать, как «краситель», «красящее вещество», «красящий пигмент». Однако на языке химии – это принципиально разные соединения. Dyes – это химическое вещество, проявляющее цвет при растворении. Более того, существуют различные по своей химической природе dye. Lakes – нерастворимое вещество, пигмент, который получают путём осаждения растворимого красителя солями металлов. К колоранту также относят micas или mica (мика или слюда). Мика тоже встречается в составе пигментов для перманентного макияжа.

Перманентный макияж является интрадермальным введением колорантов и вспомогательных ингредиентов для улучшения контуров лица. Это официальное определение из Резолюции Евросоюза ResAP (2008) 1 о требованиях и критериях безопасности татуировок и перманентного макияжа. Это основополагающий документ, который приняли в Евросоюзе из-за популярности процедур. По сути, он носит рекомендательный характер, так как общего законодательства у стран ЕС нет. На базе Резолюции Бельгия, Франция, Германия, Норвегия, Швейцария, Лихтенштейн, Словения, Испания, Швеция и Нидерланды разработали собственные нормативные акты. Производители чернил для перманентного макияжа из стран ЕС, у которых нет национального законодательства, попадают под действие Директивы 2001/95/ЕС об общих требованиях к безопасности продукции (General product safety directive – GPSD). Ряд вопросов, связанных с регистрацией химических веществ, регулируются Регламентом CLP/ Регламентом Европейского парламента и Совета ЕС 1272/2008 о классификации, маркировке и упаковке веществ и смесей CLP (Classification, Labeling, and Packaging) (EC No 1272/2008). Кроме того, их оборот контролируется Европейским агентством по химикатам (ECHA) на основании Регламента Европейского союза № 1907/2006 (REACH). Помимо перечисленных документов, европейские производители чернил для перманентного макияжа могут руководствоваться:

- Регламентом Европейского Парламента и Совета Европейского союза 1223/2009 от 30 ноября 2009 г. о косметической продукции;
- Решением Европейской комиссии 2008/721/ЕС от 5 сентября 2008 г.;
- Решением Европейской Комиссии 96/335/ЕС от 8 мая 1996 г.;
- Директивой 76/768/ЕЭС Совета ЕС от 27 июля 1976 г.

В США наряду с колорантами фигурирует дефиниция «цветовые добавки» (color additive). Федеральное регулирование цветовых добавок главным образом основано на Федеральном законе о пищевых продуктах, лекарственных средствах и косметических средствах (Federal Food, Drug, and Cosmetic Act – FD&C Act) и его поправках. Выпуск и сертификация некоторых пигментов контролируется Управлением по санитарному надзору за качеством пищевых продуктов и медикаментов (Food and Drug Administration – FDA).

Колоранты, цветовые добавки и другие ингредиенты, которые применяются при производстве пигментов, перечисляются в Международной номенклатуре косметических ингредиентов (International Nomenclature of Cosmetic Ingredients – INCI). Этот «словарь веществ» создали в США специалисты организации The Cosmetic, Toiletry, and Fragrance Association (CTFA) и опубликовали в 1973 году. В первом справочнике было всего 5000 наименований. В 2007 году организация была переименована в The Personal Care Products Council (Совет по средствам личной гигиены). Совет периодически обновляет и публикует International Cosmetic Ingredient Dictionary and Handbook. Книга доступна и в электронной версии. На официальном портале Совета можно оформить подписку. В справочнике сейчас указаны более 22 600 наименований ингредиентов, приведены ссылки на 70 00 торговых и технических названий. Доступ к базе стоит $1520. Для члена Совета талмуд обойдётся в $525. Версию списка ингредиентов разных годов можно найти в интернете бесплатно. Существуют и специальные порталы, где можно узнать вещество, зная одно из имён.

В INCI используются латынь для растительных ингредиентов и английский язык для молекул и общепринятых наименований. Сертифицированные пигменты имеют сложные и громоздкие названия, поэтому в американской классификации их могут сокращать до аббревиатур. К примеру, dyes можно обозначать, как «D&C» Colors, т. е. они могут быть в составе медикаментов и косметических средств, но никак не продуктов питания. Lakes, в свою очередь, можно указывать, как «FD&C» Colors. К примеру, у колоранта с INCI-именем Blue 1 Lake есть второе сертифицированное имя – FD&C Blue No. 1 Aluminum Lake.

Помимо INCI, у колорантов могут быть ещё и регистрационные номера CAS, EINECS и ELEINCS. Номер CAS записывается в виде трёх групп арабских чисел, разделённых дефисами. Он вносится в реестр Химической реферативной службы США (Chemical Abstracts Service). Регистрационный номер EINECS – это уникальный семизначный идентификатор, который содержится в Европейском перечне существующих химических веществ (European Inventory of Existing Commercial Chemical Substances – EINECS). Номер ELINCS указывается в Европейском перечне зарегистрированных химических веществ (European List of Notified Chemical Substances – ELINCS).

Официальной альтернативой номенклатуре INCI служит европейская система Color Index names. Красители обозначаются в соответствии с международным индексом Colour International index и выглядят как буквы CI и пятизначный числовой код. Пожалуй, поиск ингредиентов по индексу – самый простой и понятный способ. В Европейском союзе также создана официальная база данных косметических ингредиентов – EU Cosing, как разрешённых, так и запрещённых к использованию. Ресурс содержит, на мой взгляд, наиболее полную информацию с указанием имён, химической формулы, сфер применения. Искать интересующее вещество можно, как по американской INCI, так и по CI коду.

В Резолюции ResAP (2008) 1 описаны требования к упаковке и составу чернил для перманентного макияжа. Указываются имена ингредиентов согласно Международному союзу теоретической и прикладной химии (International Union of Pure and Applied Chemistry – IUPAC), регистрационный номер CAS (Chemical Abstract Service of American Chemical Society) или номер индекса цвета (CI).

Можно найти информацию, что пигменты для перманентного макияжа делают и в России. Но практически всё сырьё, понятное дело, будет привозным, если вообще не полностью субстанция. Что же касается правового поля, то пигменты для эпидермального татуажа должны отвечать требованиям технического регламента Таможенного союза ТР ТС 009/2011 «О безопасности парфюмерно-косметической продукции». Мастера должны работать в соответствии с ГОСТ Р 55700 Услуги бытовые. Косметический татуаж. Общие требования. С 1 октября 2019 года в силу вступил новый стандарт – ГОСТ Р 58391-2019 Пигменты для косметического татуажа. Требования безопасности.

Классификация и состав пигментов

Изготовление пигмента для перманентного макияжа (PMU pigment) – сложный химический процесс. Пигмент состоит из сухого красящего вещества (собственно, пигмента) и жидкой среды, т. е. проводника пигмента в кожу (rewetting agents). Если сильно упрощать описание процесса, то сырьё преобразуют в мелкодисперсную или пигментную пудру (pigment powder). Полученную массу просеивают через так называемое нано-сито с определённым размером ячейки. Затем, исходя из рецептуры, добавляют компоненты и смешивают пигмент с жидкой основой-проводником в высокоскоростных фармацевтических миксерах из нержавеющей стали.

В качестве жидкой среды, с которой будет смешиваться пигментная пудра, могут выступать глицерин (glycerin), спирт (alcohol), дистиллированная вода (distilled water). Под понятием «спирт» обычно подразумевается изопропиловый спирт (isopropyl alcohol). В зависимости от процентного содержания жидких элементов чернила для перманентного макияжа условно разделяют на водно-спиртовые, спиртовые и глицериновые. Для выполнения стойкой и яркой работы мастеру перманентного макияжа важно учитывать качество жидкой основы чернил. Информация о соотношении веществ приводится на этикетке. Компоненты перечисляются в порядке уменьшения концентрации. Считается, что пигменты с преобладающей глицериновой основой более плотные, лучше проникают в кожу, обеспечивают равномерное заживление тканей, выглядят ярче. При этом со временем под воздействием организма, внешней среды тускнеют, становятся блёклыми, что, по сути, и отвечает задачам перманентного макияжа.

Кроме базовых элементов, производители часто добавляют на стадии финального смешивания ингредиентов алоэ вера (Aloe Barbadensis), экстракт гамамелиса/дистиллят орешника вирджинской ведьмы (witch hazel/hamamelis virginiana). Он успокаивает жирную и смешанную кожу, обладает антисептическим, противовоспалительным действием. В составе чернил может присутствовать магния алюмосиликат (Magnesium Aluminum). Это хорошо переносимый с дерматологической точки зрения загуститель и стабилизатор. Таких дополнительных компонентов может насчитываться порядка 20. Наличие полезных для кожи ингредиентов стимулирует процессы регенерации тканей после процедуры. Кроме того, в составе пигментов для перманентного макияжа можно часто найти:

- Полисорбат-20 (polysorbate 20). Выступает в качестве эмульгатора и стабилизатора в составе средств на водной основе. Для его изготовления используется кокосовое масло.
- Метилпарабен (methyl paraben), пропилпарабен (propyl paraben). Это синтетические консерванты.
- Феноксиэтанол (phenoxy ethanol). Концентрация этого консерванта не должна превышать 1%.
- Поливинилпирролидон (polyvinylpyrrolidone/PVP). Это водорастворимый синтетический полимер. Его применяют для так называемого улучшения «диспергирования пигментов».
- Аммония метакрилата сополимер (ammonium methacrylate copolymer). Эмульгатор, плёнкообразователь синтетического происхождения.

С содержанием некоторых дополнительных компонентов, в особенности, так называемых полиакрилатов, может быть связано появление «расплавов» и изменение цвета при удалении или коррекции перманентного макияжа лазером или ремувером.

Самая распространённая и понятная классификация пигментов для перманентного макияжа, т. е. «сухого вещества», – это разделение на оксиды железа (iron oxide), неорганические и органические соединения. У неорганических ингредиентов «цифровая часть» CI будет начинаться с 7, у органических – с 1,5.

К неорганическим соединениям относят оксид хрома (oxide chrome), диоксид титана (titanium dioxide), пигменты ультрамариновых цветов (ultramarines), пирофосфат аммония-марганца (III) или тёмно-фиолетовый краситель (manganese violet CI 77742), оксид-хлорид висмута (bismuth oxychloride CI 77163). Их синтетическим способом получают из металлов. Наряду с указанными соединениями в состав чернил может добавляться каолин (aluminium silicate/china clay CI 77004). Основное преимущество неорганических пигментов – гипоаллергенность.

Технически, оксиды железа являются неорганическими минеральными соединениями. Но есть бренды, которые указывают, что не использует в производстве чернил для перманентного макияжа именно оксиды железа, а только органические и неорганические ингредиенты. Сейчас фактически, более 95% производимых в мире пигментов для татуажа содержат как органические, так и неорганические соединения. Красители на основе оксида железа являются базовыми пигментами для перманентного макияжа. Они входят в состав красок для татуажа бровей, губ, прорисовки стрелок на веках, для создания эффекта румян, тональной основы. Эти пигменты можно разделить на три подгруппы:

- чёрный оксид железа (black iron oxide) CI 77499.
- жёлтый оксид железа (yellow iron oxide) CI 77492.
- красный оксид железа/колькотарь (red colcothar) CI 77491.

Путем смешивания этих цветов в различных соотношениях можно получить практически любой оттенок. Они стабильно ведут себя на коже, нетоксичны. Считается, что такие пигменты легко удаляются с помощью лазера. Однако их преобладающее содержание в составе краски действительно может вызывать неравномерное выцветание, изменение цвета, появление тех самых красноватых оттенков.

В зарубежных публикациях также можно встретить классификацию неорганических пигментов в зависимости от цвета. Выделяют красные, синие, зелёные, чёрные, коричневые, белые, жёлтые пигменты. Часто используемым пигментом является чёрный углерод (carbon black) - Pigment Brown 6, 7 (CI 77266). Диоксид титана – это белый пигмент (CI 77891), который позволяет добиться более светлых оттенков. Есть утверждения, что диоксид титана может давать со временем зелёный или голубой подтон. К белому пигменту также относят сульфат бария - Barium sulphate (CI 77120). К синим

пигментам относят ультрамарин (CI 77007), прусский синий - Pigment blue 27 (CI 77510).

Часто используемым при изготовлении чернил для перманентного макияжа является оксид хрома: Pigment green 18 (CI 77289); Pigment green 17 (CI 77288). Это минеральный краситель, зелёный пигмент. Коричневый цвет получают путём смешения оксидов железа с оксидом хрома. Оттенки могут быть разными – в зависимости от содержания оксидов железа в пигменте – от цвета чайной розы до тёмного шоколада. Добавленный в краску, зеленый цвет обеспечивает оливковый тон перманентного макияжа, который натурально смотрится. Кроме того, оксид хрома является естественным стабилизатором красноты, которая может проявиться в процессе выгорания пигмента. Но тут стоит учесть, что, к примеру, использование в пигменте «красного оксида хрома» (Pigment Red 104, CI 77605) может со временем дать нежелательный красный оттенок. Не исключён и переход в зеленоватый оттенок.

Органические пигменты создаются на основе углерода в лабораторных условиях и комбинируются с различными веществами, чаще всего с азотом, водородом и кислородом. Изменяя их соотношения, производители добиваются нужного цвета. Т. е. речь идёт о синтетической органике, потому как природная запрещена к производству из-за риска аллергии на растительный или животный белок. Для создания органических пигментов используют также гидроксид алюминия. Это нерастворимая субстанция, которая «удерживает» цвет, делает пигмент стабильнее и позволяет лучше проникать в кожу. Органические пигменты считаются гипоаллергенными. Среди недостатков указывают худшее качество получаемых тёмных оттенков по сравнению со светлыми. Кроме того, пигменты на основе углерода не рекомендуют использовать для прорисовки стрелок из-за возможного изменения цвета.

Органические пигменты по сравнению с неорганическими отличают:

- широкая цветовая палитра.
- более мелкий размер частицы пигмента.
- более насыщенный цвет.
- меньшая стабильность в коже.

Из-за меньшей стабильности органические пигменты могут больше «подплывать». С учётом этой особенности их рекомендуют использовать для техник растушевки.

Органические пигменты разделяют на полициклические и азокрасители. К азокрасителям относятся вышеупомянутые lakes. К наиболее используемым колорантам для производства чернил для перманентного макияжа относятся:

- Красные – Pigment red 57:1 (CI 15850:1); Pigment red 57:2 (CI 15850:2); Pigment red 254 (CI 56110); Acid red 14, Food red 3 (Carmoisine lake) (CI 14720).
- Жёлтые – Acid yellow 104 aluminium lake (CI 15985:1); Pigment yellow 138 (CI 56300); Food yellow 3 (CI 15985); Pigment yellow 74 (CI 11741).
- Оранжевые – Pigment orange 13 (CI 21110); Pigment orange 16 (CI 21160).
- Коричневый – Pigment brown 25 (CI 12510).
- Зелёный – Pigment green 36 (CI 74265).

Согласно техническому отчёту Европейского союза 2015 года, посвящённому чернилам для татуировки и перманентного макияжа, помимо перечисленных колорантов, в состав краски для перманентного макияжа могут входить десятки других веществ, в том числе запрещённых или не рекомендованных лабораториями.

Ограниченный пигмент

Вещества, которые не должны входить в состав чернил для перманентного макияжа либо их концентрация должна быть ограничена, перечислены в уже знакомой нам Резолюции Евросоюза ResAP (2008) 1. Это ароматические амины, канцерогены, мутагенные красители, полимеризационные аморфные углеводороды (ПАУ), примеси металлов. Большинство европейских производителей избегают наименований из этого перечня. При этом использование отдельных ингредиентов может быть ограничено ещё и национальным законодательством.

В начале 2020 года Европейского агентство по химикатам заявило о намерении ограничить использование более 4 тысяч субстанций для производства чернил для перманентного макияжа. При этом в Евросоюзе остаётся открытым вопрос согласования аналитических методов определения содержания никеля. Согласно Резолюции, его содержание должно быть минимальным, насколько это технически возможно, исходя из рецептуры получаемого вещества. Схожая проблема касается и лабораторного определения ПАУ, канцерогенных ароматических аминов.

При этом в США, Управление по санитарному надзору за качеством пищевых продуктов

и медикаментов выдвигает к производителям свои требования. В перечне цветовых добавок, не подлежащих сертификации: manganese violet, зелёный оксид хрома (CI77288); оксид железа (CI 77491); диоксид титана (CI77891), мика. В свою очередь, синтетические органические колоранты подлежат тестированию и сертификации.

Дискуссии и разногласия относительно влияния того или иного пигмента возникают из-за отсутствия масштабных научных исследований, общего законодательства, единого для всех стран мира списка запрещённых веществ. Как потребители чернил для перманентного макияжа, мы не можем полностью предсказать их поведение, так как не знаем всю рецептуру и концентрацию отдельно взятого ингредиента. Это должен, в принципе, понимать и сам клиент. Ведь на поведение пигмента и цветовой результат будут также влиять:

- Цвет кожи (тон и подтон).
- Плотность и строение кожи.
- Скорость процессов восстановления.
- Стабильность колоранта.
- Цвет выбранного пигмента.
- Глубина введения пигмента.

Соответственно, мастер перманентного макияжа может научиться «читать» состав ингредиентов на флаконе с чернилами, стараться на основе своего опыта грамотно выбирать пигмент, но полностью спрогнозировать изменение цвета не получится.

ORLOVA Elsa
master of permanent makeup of international class,
Concept Line, USA, Boca Raton

THE INTRODUCTION OF PIGMENT: IS IT POSSIBLE TO PREDICT COLOR CHANGES?

Abstract. *The article discusses in detail the issues related to the introduction of pigment into the skin in the context of permanent makeup and pigment color changes after the procedure. The influence of various factors, including the quality of the pigment, the composition of the ingredients and the external conditions, on the final result of the procedure is described. The main focus is on the chemical composition of pigments, their classification, as well as legislative and regulatory acts regulating their use in different countries. The role of the pigment manufacturer and the need for permanent makeup artists to understand the pigment composition in order to predict and minimize possible color changes are discussed.*

Keywords: *pigment introduction, permanent makeup, pigment color change, chemical composition of pigments, pigment classification, legislation and regulations, pigment quality, pigment manufacturers, factors influencing color, pigment composition analysis.*

ФИЛОЛОГИЯ, ИНОСТРАННЫЕ ЯЗЫКИ, ЖУРНАЛИСТИКА

КУЛИК Елена Анатольевна
учитель иностранных языков,
ОГБОУ «Валуйская СОШ №4», Россия, г. Валуйки

ПОВЫШЕНИЕ ПЕДАГОГИЧЕСКОЙ КОМПЕТЕНТНОСТИ И ТВОРЧЕСКОЙ АКТИВНОСТИ ПЕДАГОГОВ ЧЕРЕЗ ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ КРИТИЧЕСКОГО МЫШЛЕНИЯ (ЗАОЧНЫЙ МАСТЕР-КЛАСС)

Аннотация. *В статье повышение педагогической компетентности и творческой активности педагогов через использование технологии критического мышления рассматривается в качестве одного из приоритетных направлений в любой образовательной деятельности, которая направлена на развитие индивидуальности ученика.*

Ключевые слова: *ТРКМ (технология развития критического мышления), творческая активность, приёмы, практический опыт.*

Повышение педагогической компетенции и творческой активности педагогов – одно из важных условий реализации ФГОС. В своей педагогической деятельности на уроках английского языка я стараюсь делать акцент на гибкости, критичности мышления. Почему критическое? В огромном потоке информации современного мира оно является необходимым в учебе, работе и нашей повседневной жизни. Критическое мышление – это способ мышления, при котором человек ставит под сомнение поступающую информацию, собственные убеждения. Исходным условием всесторонне развитой личности является социальный заказ общества на обеспечение качества гуманитарного образования. Другим условием возникновения и становления является потребность современного общества в образованной личности, умеющей строить диалог со всеми субъектами общего жизненного пространства. Владение иностранными языками – не только аспект культурного развития человека, но и обязательное условие его успешной деятельности в самых различных областях. Определяющим условием является стремление к совершенствованию учебно-воспитательного процесса в ОГБОУ «Валуйская СОШ №4» Белгородской области и собственный интерес к обозначенной проблеме.

Дайана Халперн, американский психолог, отмечает критическое мышление как творческое, развивающее обучение, которое учит мыслить рационально. Это способность анализировать информацию с позиции логики. Если это не верно, то, что верно? Если допущена ошибка, как ее исправить? С какой целью написан этот текст? К какой аудитории обращается автор? Я хочу продемонстрировать вам некоторые методические приемы технологии критического мышления. Я думаю, что вы все используете их в своей работе, ведь они универсальны. Их можно применять не только на уроках, занятиях, но и любых других подобных мероприятиях (семинары, рабочие встречи, педсоветы и т. д.). Технология критического мышления состоит из следующих стадий (рис. 1).

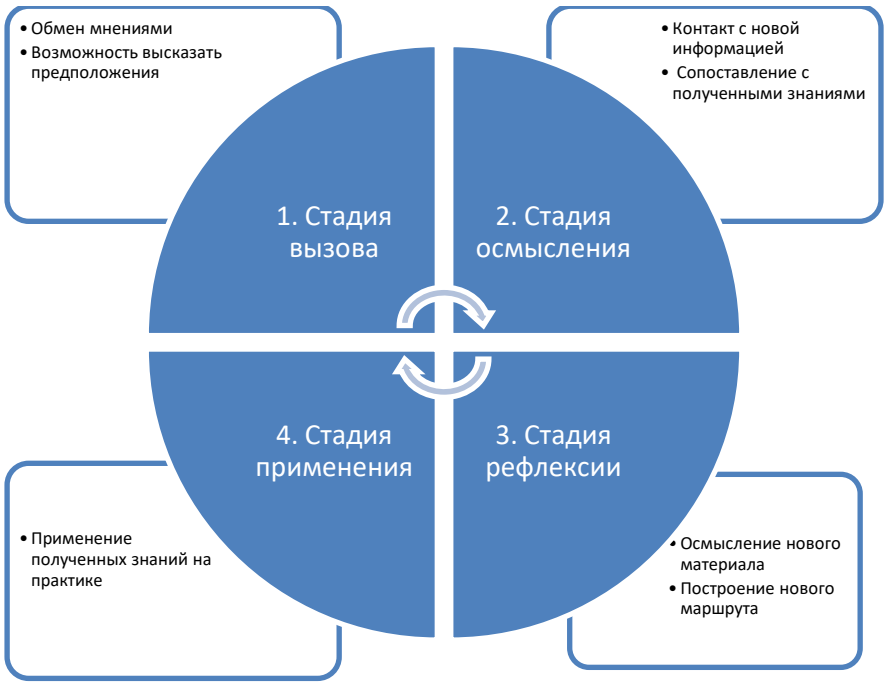


Рис. 1. Образовательная технология критического мышления

Приём, который называется **«Тонкие и толстые вопросы…»** (таблица) этот приём используется на стадии вызова с последующим установлением истины на стадии рефлексии.

Таблица

Приём «Тонкие и толстые вопросы»

Толстые вопросы	Тонкие вопросы
Объясните, почему…?	Кто…?
Почему вы считаете…?	Что…?
Предложите, что будет, если…?	Когда…?
Смогу ли я…?	Могут ли…?
Дайте три объяснения, почему…?	Верно, ли…?
Почему вы думаете…?	Будет…?

Особенно важно научиться задавать друг другу открытые вопросы, которые побуждают размышлять, думать, воображать, творить или тщательно анализировать.

Приём: «Лови ошибку»

Например: Рибята пришли в лез. У пенка лижал ёш. По трапинке прополс уж. Вдруг надвинулась тучя. Пошёл дожть. Мы побижали домой.

Find the mistake, if there is one here (Найдите ошибку, если она есть).

Один из вариантов:

- fifteen minus six equals five.
- twenty-seven minus x equals nineteen. If x equals five.
- eighty-two plus eleven equals one hundred.

Один из вариантов:

A hedgehog is a bird. (an animal).

Dinner is a meal.

Big Ben and Tower are building materials. (the landmarks)

Cotton is a plant.

Beds, sofas, tables are the food.

Apples and pears are animals.

Gagarin is an astronaut.

Cars, lorries and buses are transport.

1) Демонстрация рисунка, фотографии, картинки

2) Описание увиденного, высказывание своих предположений

3) Составление описательного минитекста

Рис. 2. The Picture Word Inductive Model

Приём: «Доска вопросов»

«Доску вопросов» можно поместить в легкодоступном месте. Когда у учителя нет времени ответить на все вопросы, ученики могут их там записать, и учитель может потом их собрать, выучить и ответить или в письменной форме, или устно на следующих уроках, или вынести их на обсуждение в классе.

Приём: «Игра слов»

Используя данный приём, можно придумать для своих коллег (учеников) вопросы и дать им категории на любые темы: название стран, профессий, числительные, цвет, месяц, дни недели и т. д.

- Pam is a: a) surname b) first name c) girl's name.
- Russia is a: a) language b) nationality c) country.

Приём: «Синквейн»

Синквейн – это «стихотворение», состоящее из 5 строк. При этом каждая строка подчинена определенным правилам. Происходит, таким образом, подведение итогов по изученному материалу. Синквейн способствует активизации умственной деятельности.

The first line. **Family.**

Second line. (What is a family look like?) *strong, friendly*

We can choose only two adjectives.

The third line. What a person does in a family? *love, help, respect*

Fourth line *I love my family.*

Fifth line. One word here is a synonym. **Dynasty** (или дом) house.

На самом деле приёмов критического мышления очень много и структура нетрадиционного урока зависит от нашей педагогической компетентности и творческой активности.

При использовании технологии развития критического мышления педагог перестает быть главным источником информации и превращает обучение в совместный поиск, что даёт положительные преимущества:

- есть возможность повторения, лучшего усвоения материала;
- вырабатывается уважение к собственным мыслям и опыту;
- развивается любознательность, наблюдательность;
- дети становятся более восприимчивы к опыту других ребят, они учатся слушать друг друга, несут ответственность за совместный способ познания;
- в ходе обсуждения появляются несколько трактовок одного и того же содержания;
- исчезает страх перед белым листом и перед аудиторией;
- предоставляется возможность в процессе рассуждений, сделать правильный вывод;

Благодаря применению педагогом ТРКМ, дети легко и быстро усваивают материал, необходимый для подготовки к школьному обучению, повышается учебная мотивация. Органичное включение творческих заданий в систему школьного образования, даёт возможность личностного роста ребенка, ведь такая работа обращена, прежде всего, к его индивидуальности.

KULIK Elena Anatoljevna
Teacher of foreign languages,
Main state budget-funded educational institution «Valuyskaya SOSH No.4»,
Russia, Valuiki

IMPROVING PEDAGOGICAL COMPETENCE AND CREATIVE ACTIVITY OF TEACHERS THROUGH THE USE OF CRITICAL THINKING TECHNOLOGY

Abstract. *In the article the increase of pedagogical competence and creative activity of teachers through the use of critical thinking technology is considered as one of the priority directions in any educational activity.*

Keywords: *critical thinking technology, creative activity, techniques, practical experience.*

КУЛЬТУРОЛОГИЯ, ИСКУССТВОВЕДЕНИЕ, ДИЗАЙН

РАХИМОВ Сердар
студент, Казанский (Приволжский) федеральный университет,
Россия, г. Казань

РАЗВИТИЕ КУЛЬТУРНО-ПОЗНАВАТЕЛЬНОГО ТУРИЗМА В ТУРКМЕНИСТАНЕ

Аннотация. *Статья посвящена исследованию инновационных подходов к развитию туризма в Туркменистане. В современном мире туризм является важным фактором экономического развития многих стран, и Туркменистан, обладающий богатым культурным и природным наследием, стремится активно развивать свою туристическую индустрию. В статье рассматриваются различные инновационные подходы, которые могут способствовать развитию туризма в Туркменистане. Особое внимание уделяется использованию информационных технологий, таких как онлайн-платформы и мобильные приложения, для улучшения доступа туристов к информации о достопримечательностях, бронированию и планированию поездок. Также рассматривается создание устойчивых туристических маршрутов и развитие современной инфраструктуры, включая транспортные сети и гостиничное хозяйство. Статья также анализирует опыт других стран, успешно применяющих инновационные подходы в сфере туризма, и выделяет ключевые уроки, которые могут быть применимы в контексте Туркменистана. Особое внимание уделяется привлечению инвестиций в туристическую индустрию и созданию партнерств с международными инвесторами. Результаты исследования позволяют сделать выводы о потенциале инновационных подходов для развития туризма в Туркменистане и предлагают рекомендации для правительства и туристических компаний по их внедрению. Статья имеет практическую значимость для разработки стратегии развития туризма в Туркменистане и может быть полезной для специалистов и исследователей, занимающихся этой темой.*

Ключевые слова: *международный туризм, национальная туристическая зона, конкурентоспособный туристический комплекс.*

Введение

Туризм является важной отраслью для экономического развития многих стран, включая Туркменистан. Для привлечения большего числа туристов и стимулирования роста туристической индустрии необходимо использовать инновационные подходы. В данной статье будет рассмотрено развитие туризма в Туркменистане и представлены инновационные стратегии, которые могут способствовать его развитию. Будут рассмотрены примеры успешных международных моделей и предложены рекомендации для применения в контексте Туркменистана. Целью данной статьи является исследование и анализ инновационных подходов к развитию туризма в Туркменистане с целью привлечения большего числа туристов и увеличения экономической выгоды для страны.

Актуальность исследования. Туркменистан обладает богатым наследием и уникальными природными достопримечательностями, такими как пустыня Каракум, горы Копетдаг, исторические города Мерв и Ниса, а также богатой культурой и традициями. Однако, несмотря на это, потенциал туризма в стране остается недостаточно развитым, что делает актуальным исследование инновационных подходов для его активации и привлечения большего числа туристов

Методы. Этот метод включает сбор и анализ данных о текущем состоянии туризма в Туркменистане. Это может включать данные о посещаемости, доходах от туризма, основных

туристических достопримечательностях и т. д. Анализ этих данных поможет понять сильные и слабые стороны туристической индустрии и определить области, требующие инновационных подходов.

Обзор литературы. Инновационные подходы к развитию туризма в Туркменистане привлекают все большее внимание исследователей и практиков. В литературе можно найти ряд работ, которые исследуют различные аспекты развития туризма в стране и предлагают инновационные подходы для его усиления. Вот несколько ключевых исследований:

«Развитие туризма в Туркменистане: вызовы и перспективы» (автор: Ахмедов А. А.) – данное исследование рассматривает основные вызовы, с которыми сталкивается туризм в Туркменистане, и предлагает стратегии для их преодоления. Автор также обсуждает важность инноваций в развитии туризма и предлагает некоторые конкретные меры для их реализации.

«Инновационные технологии в туризме: опыт и перспективы для Туркменистана» (автор: Ибрагимова Г. Х.) – это исследование фокусируется на использовании информационных технологий в туризме и их роль в привлечении туристов в Туркменистан. Автор предлагает использовать онлайн-платформы и мобильные приложения для предоставления информации и услуг бронирования туристам.

«Инновационные стратегии развития туризма в Центральной Азии» (автор: Жумабаева Д. М.) – данное исследование рассматривает не только Туркменистан, но и другие страны Центральной Азии. Автор выделяет важность развития устойчивых туристических маршрутов, инфраструктуры и привлечения инвестиций для развития туризма в регионе.

«Туристический потенциал Туркменистана и его использование в инновационных стратегиях» (автор: Караева Л. М.) – в этом исследовании автор анализирует туристический потенциал Туркменистана, включая его природные и культурные достопримечательности. Он предлагает использовать инновационные подходы, такие как развитие экотуризма и создание туристических маршрутов, чтобы привлечь больше туристов.

Эти исследования представляют лишь небольшую часть литературы, посвященной инновационным подходам к развитию туризма в Туркменистане. Они подчеркивают важность использования новых идей и стратегий для привлечения туристов и стимулирования роста туристической индустрии в стране.

Результаты и обсуждение

Расширение потенциала национального туристического сектора является одним из приоритетов социально-экономической политики независимого и нейтрального Туркменистана. В настоящее время в стране действует более 20 государственных и индивидуальных туристических предприятий, которые ежегодно обслуживают более 70 тысяч туристов, в том числе около 30 тысяч иностранных туристов примерно из 60 стран мира. На сегодняшний день заключено более 150 соглашений с зарубежными туристическими компаниями о сотрудничестве в сфере туризма.

Важным аспектом развития туристического комплекса в нашей стране является позитивное сотрудничество со Всемирной туристской организацией ООН (UNWTO). Туркменистан принимает активное участие в различных мероприятиях, организуемых этой крупнейшей в мире международной организацией. В свою очередь, руководители Всемирной туристской организации оказывают посильную помощь нашей стране в плане развития отрасли. «Национальная программа поддержки и развития туристического сектора Туркменистана на 2011–2020 годы», принятая непосредственно под руководством уважаемого Президента Туркменистана Гурбангулы Бердымухамедова, получила высокую оценку и поддержку Всемирной туристской организации. Как указано в этом документе, главной стратегической целью развития рекреационного сектора является создание высокоэффективной и конкурентоспособной индустрии туризма в Туркменистане. Расширение географии туристических маршрутов, формирование национального туристического комплекса, соответствующего современным рыночным отношениям и учитывающего мировой опыт в этой сфере, оказывают стимулирующее воздействие на развитие других отраслей экономики страны, популяризацию культурного и природного наследия страны, которое, в конечном счете, способствуют значительному увеличению числа иностранных туристов и валютных поступлений, создавая условия для реализации туристических проектов различного масштаба.

Инициатива Президента Туркменистана по созданию национальной туристической зоны «Аваза» на восточном побережье Каспийского моря является поистине инновационной, она

означает принципиально новые подходы к реализации огромного природного и экономического потенциала страны [2, с. 6]. Этот грандиозный проект называют одновременно чудом туркменской земли и символом всех грандиозных перемен, произошедших в Туркменистане в эпоху могущества и счастья. «Аваза» – беспрецедентный проект для страны как с точки зрения масштабов строительства и высокого интереса к нему иностранных туристов, так и с точки зрения перспектив, которые он открывает для развития рекреационного сектора. Морские круизы, яхты, дайвинг, полеты на параплане, виндсерфинг и другие водные виды спорта дополняют проживание в многочисленных современных отелях, виллах и уютных коттеджах. Для развития экологического аспекта в прибрежной туристической зоне одним из перспективных направлений энергосбережения является использование солнечной энергии. По мнению экспертов, оптимизация систем электроснабжения должна основываться на принципах сочетания альтернативных и традиционных источников сырья с учетом сезонных и суточных графиков потребления энергии. В прибрежном проекте коттеджный городок Союза промышленников и предпринимателей страны предусматривает установку солнечных панелей для преобразования световой энергии солнца в электричество. Вырабатываемый избыток электроэнергии накапливается в мощных аккумуляторах и может использоваться как ночью, так и в пасмурную погоду. Таким образом, применение научно обоснованных подходов и инновационных методов при выполнении строительных работ обеспечивает дальнейшее устойчивое эколого-экономическое развитие национальной туристической зоны «Аваза».

Городские поселения также являются важной частью культурных и рекреационных ресурсов, привлекающих иностранных туристов. Ашхабад – столица и крупнейший город страны с крупнейшим международным аэропортом в Центральной Азии, расположен в предгорьях Копетдага, административно имеет статус столичного велаята (области). В городе активно внедряется инновационная градостроительная концепция, направленная на создание здесь национальной культурной и рекреационной среды. Преобразование архитектурного облика столицы путем строительства многоэтажных зданий, облицованных белым мрамором, осуществляется параллельно с использованием величественных скульптурных форм. В оформлении городского ландшафта значительное место отводится зеленым насаждениям и фонтанным комплексам. Строительство грандиозного спортивного комплекса в Ашхабаде – Олимпийском городке – включает в себя возведение более 30 уникальных спортивных и других объектов для проведения здесь в 2017 году V Азиатских игр в закрытых помещениях и по боевым искусствам. Азиатские игры 2017 года, несомненно, сыграют значительную роль в продвижении международного спортивного туризма в стране.

Туркменистан обладает богатым духовным и культурным наследием. Сохранившиеся архитектурные памятники свидетельствуют о значительном былом культурном и экономическом могуществе туркменского народа, сохранению которого государство уделяет приоритетное внимание [3, с. 24]. Именно историческая и культурная самобытность и национальное наследие, включая всемирно известные туркменские ковры и ахалтекинских скакунов, являются фактором повышения международного рейтинга в этом секторе, завоевания все более значимых позиций на мировом туристическом рынке.

Таким образом, реализация стратегии развития туризма в Туркменистане создает условия для дальнейшей успешной интеграции страны в мировой туристический рынок.

Литература

1. Воронов Ю.П., Суслов В.И. Воздействие туризма на другие отрасли экономики. // Устойчивое развитие туризма: опыт и инновации: межд. конф. (Улан-Удэ, 23–25 мая 2007). Улан-Удэ: Изд-во БНЦ СО РАН, 2010. С. 27-36.

2. . Бердымухамедов Г. Нейтральный Туркменистан. Ашхабад, 2015. 240 с.

3. Медведева М.Н. Оценка рекреационных ресурсов Туркменистана для организации отдыха в аридных условиях. Автореф. канд. геогр. наук. Ашхабад, 1983, 34 с.

4. "Tourism Development in Central Asia: Challenges and Opportunities" by R. Sharpley and D. J. Telfer.

5. "Tourism Innovation: Technology, Sustainability and Creativity" by M. M. Carvalho and A. S. Marques.

6. "Tourism and Innovation: Contemporary Geographies of Leisure, Tourism and Mobility" edited by C. Michael Hall, Jarkko Saarinen, and Dieter K. https://books.google.kz/books?id=-

LF8AgAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

7. Отчеты и публикации международных организаций: Международные организации, такие как Всемирная туристическая организация (UNWTO) и Международный фонд по развитию сельского хозяйства (IFAD), https://www.unwto.org/search?keys=turkmenistan.

RAKHIMOV Serdar
student, Kazan (Volga Region) Federal University, Russia, Kazan

DEVELOPMENT OF CULTURAL AND EDUCATIONAL TOURISM IN TURKMENISTAN

Abstract. *The article is devoted to the study of innovative approaches to the development of tourism in Turkmenistan. In the modern world, tourism is an important factor in the economic development of many countries, and Turkmenistan, which has a rich cultural and natural heritage, strives to actively develop its tourism industry. The article discusses various innovative approaches that can contribute to the development of tourism in Turkmenistan. Special attention is paid to the use of information technologies, such as online platforms and mobile applications, to improve tourists' access to information about attractions, booking and planning trips. The creation of sustainable tourist routes and the development of modern infrastructure, including transport networks and the hotel industry, are also being considered. The article also analyzes the experience of other countries that successfully apply innovative approaches in the field of tourism and highlights key lessons that can be applied in the context of Turkmenistan. Special attention is paid to attracting investments in the tourism industry and creating partnerships with international investors. The results of the study allow us to draw conclusions about the potential of innovative approaches for the development of tourism in Turkmenistan and offer recommendations for the government and travel companies on their implementation. The article has practical significance for the development of a tourism development strategy in Turkmenistan and may be useful for specialists and researchers dealing with this topic.*

Keywords: *international tourism, national tourist zone, competitive tourist complex.*

ПОЛИТОЛОГИЯ

АФОНИН Андрей Александрович
старший преподаватель,
Дальневосточный федеральный университет, Россия, г. Владивосток

ПАТРИОТИЗМ КАК ФАКТОР ПОЛИТИЧЕСКОЙ ЖИЗНИ СОВРЕМЕННОЙ РОССИИ НА ПРИМЕРЕ МЕДИЙНОГО ПРОСТРАНСТВА

Аннотация. *Статья рассматривает тему трансляционных практик патриотизма в политическом медиапространстве современной России. Автор исследует способы, средства и механизмы, с помощью которых патриотические идеи и ценности передаются через различные медийные каналы и форматы. Особое внимание уделяется роли государственных и негосударственных акторов в процессе формирования и распространения патриотических настроений среди населения. В статье рассматриваются различные стратегии и тактики использования медиа для укрепления национального самосознания и увеличения гражданской активности. В статье анализируется дискурс патриотизма в контексте влияния различных конфликтогенных факторов развития современного российского политического процесса и с целью изучения технологий поддержания гражданского согласия в условиях этнополитического разнообразия. Актуализируется комплексная проблематика патриотизма как ценностного феномена политической жизни общества. Обосновывается процессуальность дискурсивного конструирования политической реальности, а также аксиологическая содержательность дискурс-анализа как метода политологии. Статья посвящена актуальной на сегодняшний день проблеме дезинформации в политическом процессе. В ходе исследования автор приходит к выводу, что наиболее значительное умение журналиста заключается в объективном оценивании событий и явлений.*

Ключевые слова: *патриотизм, медиапространство, дискурс, интернет, политика.*

На протяжении всей истории патриотизм неизменно занимал значительное место в различных аспектах жизни общества, включая духовность, экономику, политику, общество и культуру. Оно служит краеугольным камнем государственности и имеет решающее значение для эффективного функционирования социальных и государственных структур. По сути, остается вопрос: что представляет собой патриотизм и как он влияет на российское общество?

Понятие патриотизма имеет разнообразную интерпретацию, имеющую корни в греческих терминах, таких как «Патриоты» и «Патрис». На протяжении всей истории патриотизм развивался в различных социальных и ценностных контекстах, всегда связанных с такими понятиями, как «Отечество» и любовью к своей стране. Известный писатель Н. М. Карамзин разделил патриотизм на три компонента: физическую привязанность к месту рождения, социальную связь через права и обязанности и политическую преданность идеалам нации.

В настоящее время патриотизм выступает в качестве морального и политического руководящего принципа, включающего любовь к своей стране и готовность ставить интересы государства выше личных интересов. Это демонстрируется через гордость за национальные достижения, сохранение культурной самобытности и защиту родины и ее народа. Однако в наше время появляются такие понятия, как «русофобия», «антипатриотизм» и «ложный патриотизм». В этой статье рассматриваются причины этих явлений и предлагаются потенциальные меры противодействия.

Специальная военная операция по «демилитаризации» и «денацификации» Украины была объявлена президентом России Владимиром Путиным 24 февраля 2022 года. Целью этой операции преследуется защита мирных граждан, восстановление правопорядка, обеспечение мира на территории ДНР и ЛНР, а главная

задача остановить геноцид наших соотечественников, который продолжался более 8 лет: «Уверен, что преданные своей стране солдаты и офицеры Вооруженных Сил России профессионально и мужественно исполнят свой долг. Не сомневаюсь, что слаженно и эффективно будут действовать все уровни власти, специалисты, отвечающие за устойчивость нашей экономики, финансовой системы, социальной сферы, руководители наших компаний и весь российский бизнес. Рассчитываю на консолидированную, патриотическую позицию всех парламентских партий и общественных сил» [1].

На все предложения по мирному урегулированию конфликта был дан отказ, а ранее достигнутые договоренности не соблюдались. Российская сторона предлагала создать новую глобальную архитектуры безопасности, которая учитывала бы интересы граждан и обеспечивала мир и порядок. На одном из Советов Безопасности президент Российской Федерации Владимир Путин призвал выработать решение о признании Луганской и Донецкой республик суверенными, дружественными нашему государству республиками: «Военная машина, заточенная на Россию у нас под боком, нас не устраивает нацистское деление людей на сорта, что сложилось в Киеве. Исторический опыт говорит, что денацификация может быть лишь принудительной, силовой. И проводится она только извне. Собственно, сейчас это и началось. Россия берет на себя этот труд – в очередной раз вытравить из Европы нацизм. К сожалению, без посторонней помощи. Но справимся» [2].

Военная журналистика оказывает основное влияние в современных информационно-пропагандистских операциях, демонстрируя тексты, направленные на поддержку пропагандистских усилий Российского и Советского государства.

Историю нашей страны серьезно искажают и не уважают, особенно с точки зрения советской эпохи. Ставятся под сомнение героические поступки и жертвы в годы Великой Отечественной войны, игнорируется вклад миллионов людей в мирное время. Последние фильмы имеют тенденцию преуменьшать решающую роль Советского Союза в победе над фашизмом во Второй мировой войне, часто предполагая, что победа была достигнута главным образом благодаря усилиям союзников, особенно Соединенных Штатов. В таких изображениях упускается из виду, что на советско-германский фронт пришлось 75% потерь, понесенных нацистскими войсками во время войны. Настораживает тот факт, что эти фильмы производятся не только в Европе и США, но и внутри нашей страны [3, с. 330-342].

Такие исторические личности, как И. В. Сталин, Петр I, Иван Грозный, Владимир Святославич, в средствах массовой информации часто изображаются негативно, акцентируя внимание исключительно на их недостатках и проступках. Такое одностороннее освещение может привести к ошибочному восприятию прошлого и породить антипатриотизм из-за незнания истории своей страны.

Одной из причин упадка патриотических настроений является повсеместная неграмотность, особенно среди молодежи. Несмотря на то, что ежегодно российские университеты заканчивают около 900 тысяч студентов, многие из них не имеют даже базового понимания истории России. Это негативное развитие событий объясняется превращением образования в коммерческую отрасль. Однако отсутствие исторических знаний вкупе с потребительским поведением в обществе заводит в тупик.

Конечно, на более высоких уровнях продолжаются дискуссии по поводу этих проблем. В 2013 году В. В. Путин предложил разработать учебники истории с последовательным подходом, авторитетной оценкой фактических событий, без двусмысленности и на понятном русском языке. Тем не менее эта инициатива сегодня остается нереализованной, что указывает на необходимость реформы системы образования, прежде чем сосредоточиться на учебных материалах.

Проблема патриотизма тесно переплетается с проблемой оттока интеллектуальной элиты нации. После Октябрьской революции начался целенаправленный демонтаж русской культуры. Большевистская диктатура искала послушную интеллигенцию из рабочего класса, исключая инакомыслящих. Среди вынужденных покинуть страну оказались видные деятели культуры и искусства, а также известные ученые и технологи. Первая волна русской эмиграции с 1917 по 1940 год породила трёх нобелевских лауреатов: И. А. Бунина, В. В. Леонтьева и И. Р. Пригожина [6, с. 44-52].

Хотя российских граждан в настоящее время не принуждают покидать страну, а свобода слова защищена Конституцией России, существует устойчивая тенденция эмиграции

талантливых людей из-за отсутствия общественного спроса на научные достижения, а не просто недостаточного финансирования отечественная наука. В 2016 году Евростат сообщил, что 73,8 тысячи жителей России получили долгосрочный вид на жительство в ЕС, причем многие высококвалифицированные специалисты покинули страну на пике своей карьеры.

О каком патриотизме может идти речь, если важной проблемой последнего десятилетия является нерегулируемый приток масс из Центральной Азии, Южного Кавказа и Китая, которые, проживая в России, не проявляют особого интереса к ассимиляции с местным сообществом? Неконтролируемая миграция может привести к сценарию, в котором большая часть работающего населения будет состоять из низкоквалифицированных иммигрантов, что будет препятствовать инновационному прогрессу в стране. Более того, усиление миграции способствует ухудшению уровня образования и культуры. В столичных школах есть классы, в которых дети-мигранты составляют значительную часть учащихся и не владеют государственным языком.

Образование играет решающую роль в воспитании патриотизма. Однако патриотическое воспитание за последнее столетие было искажено из-за господствующих идеологий. В советское время была попытка стереть дореволюционную историю, а сейчас в современной России идет критика советского прошлого, что тормозит развитие патриотизма. Ситуация усугубляется экономическим неравенством, отсутствием инвестиций в развитие страны со стороны чиновников и общим нежеланием граждан жертвовать ради своей нации. Опросы показывают, что только 59% россиян готовы защищать свою страну военным путем, что ниже, чем в некоторых других странах.

Конечно, можно утверждать, что эта тенденция вытекает непосредственно из политики 90-х годов после распада советской социальной системы и появления рыночных отношений посредством «шоковой терапии». Продолжающийся кризис в российской экономике на протяжении последних двух десятилетий подчеркивает необходимость реальных действий со стороны правящей элиты для любого позитивного развития. Для сравнения: к середине 1930-х годов СССР уже стал ведущей европейской державой и второй мировой державой по ВВП после США. Успехи в послевоенную эпоху, такие как освоение космоса и конфронтация с Западом во время холодной войны, были заметными.

Во время войны в прессе сообщалось о военных мифах, формирующих уникальную ментальную структуру, находящуюся под влиянием экстремальных обстоятельств. Исторические события рассматривались через мифическую призму, влияя на восприятие людей. Медиацентричный подход фокусировался на том, как информация влияет на читателей и формирует мифические убеждения. Антропоцентрическая точка зрения делала упор на крайнее мифостроение, желания аудитории и потребности военного времени. Великая Отечественная война заменила довоенные политические ритуалы военными обычаями, однако национальная мифология сохранялась из-за тяжести ситуации.

В истории не бывает контрацепции, прошлое произрастает в настоящем. Годы поменяли профессиональную, духовную, гражданскую составляющую творческой интеллигенции Российской Федерации. Пропагандистскую составляющую Спецоперации представляют и транслируют ведущие журналисты медийных каналов: Александр и Андрей Коц, Дмитрий Стешин, Роман Польшаков, Евгений Поддубный, Антон Степаненко, Александр Сладков, Александр Сафиулин, Геннадий Дубовой и др. В послужных списках военкоров Косово, Афганистан, Северный Кавказ, Сирия, Египет, Украина, Нагорный Карабах, Ирак, Египет, Тунис, Ливия и др.

Военные репортеры передают тексты, вдохновляющие на храбрость и пропитанные уникальным чувством юмора. Они раскрывают правду о войне с примесью цинизма из-за эмоциональных потерь от насилия, смерти и обмана. СМИ формируют политическое влияние, направляя внимание общественности и правительства. Информационная война в спецоперациях сложна и зависит от трех десятилетий воздействия на украинских граждан. В этом контексте эксперты выделяют четыре ключевых направления:

1) работа с собственным населением;

2) работа с противником, с его армией его населением;

3) работа на мировую (слепо-немо глухую) общественность;

4) разоблачение фейков [5, с. 374-379].

Медиа в этой ситуации призваны создавать эмоциональный эффект и информировать правдой. Слоган военной кампании: «Дьявол –

спринтер, а Бог – 6 марафонец». Расшифровывается: «война правдой» – это долгая игра, но результат гораздо крепче.

В отличие от Украины, в России проблем с доступом к информации нет. YouTube доступен, Facebook, считающийся экстремистской организацией, запрещен в России, а Telegram остается неконтролируемым. Вовлечь украинскую аудиторию в информационную битву сложно из-за психологической обусловленности, которая приводит к ограниченному восприятию альтернативной информации местным населением.

Западная аудитория так же изолирована от различных точек зрения, как и украинская. Основное внимание, как правило, уделяется личным удобствам, таким как автомобили, бензин, диета и финансовая стабильность. Мало кто в России наивен, если не считать так называемой «пятой колонны». Есть история Ольги, поэтессы из Артема, которая уехала в Грузию с небольшими деньгами и псориазом, отражая решение отказаться от жизни в России. Несмотря на первоначальную поддержку, ресурсы истощились. На фоне личных проблем призывы о помощи становятся обычным явлением, подчеркивая необходимость сочувствия и критического мышления в эгоцентричном мире [4, с. 347-351].

Раскрытие лжи и дезинформации, например, сфабрикованных новостей, известных как «фейковые новости», может ввести в заблуждение аудиторию несмотря на то, что ложь легко идентифицировать и подтвердить. Например, вводящее в заблуждение сообщение из Украины о взрыве на театре военных действий раскрывает роль батальона «Азов» в инциденте, хотя первоначальные предположения были неточными.

В заключение важно подчеркнуть, что современные тенденции глобализации и европеизации постепенно ведут Россию к упадку социокультурных ценностей, что приводит к снижению чувства патриотизма и апатии среди ее граждан относительно будущего своей нации. Этот сдвиг в первую очередь связан с трансформацией основных ценностей в 1990-е годы. Устоявшиеся ценности, такие как любовь к Родине, чувство долга перед Отечеством и беззаветное служение стране, утратили свое значение среди россиян, уступив место материальным благам, отстаиваемым либеральными идеологиями. Экономическое процветание начало перевешивать духовное богатство, что особенно заметно в системе ценностей молодого населения; коллективизм уступил место индивидуализму, сопереживание сменилось эгоцентризмом. Традиционные социальные основы, такие как любовь, семья и воспитание детей, были отодвинуты на второй план в пользу материализма, сексуального поведения и нетрадиционных браков. Жить потребителем стало модно, предполагая, что все, включая любовь, дружбу и верность родине, можно купить, тем самым уменьшая мотивацию жертвовать ради общего блага нации. Понятия патриотизма, памяти предков и национальной истории были вытеснены общим западным влиянием.

Граждане России должны отстаивать свою уникальность, возрождать национальную идентичность и получать государственную поддержку посредством широкой культурной пропаганды. Понимание истории имеет решающее значение из-за ее циклического характера, позволяющего избежать прошлых ошибок. Как сказал Александр III: «Единственные союзники России – это ее армия и флот» [5, с. 374-379].

Современная журналистика, новые средства массовой информации и современные источники информации являются важнейшими компонентами военных операций, особенно в неспокойные времена. Ключевые журналистские навыки включают объективную оценку текущих событий, формирование информированного и непредвзятого мнения. Оперативная тактика, такая как дезинформация, вводит противников в заблуждение относительно реальных условий, в то время как манипуляция незаметно меняет мысли и отношения получателей. Слухи и мифотворчество возникают, чтобы повлиять на общественное восприятие во времена дефицита информации. Информационные каналы используются для вплетения мифов в ткань исторического и политического повествования страны, формирования восприятия посредством положительного и отрицательного содержания для управления конкретными процессами и событиями.

Литература

1. Владимир Путин объявил о начале специальной военной операции в связи с ситуацией в Донбассе [Электронный ресурс]. – Режим доступа: https://www.1tv.ru/news/2022-02-24/421583-
vladimir_putin_ob_yavil_o_nachale_spetsialnoy_v

oennoy_operatsii_v_svyazi_s_situatsiey_v_donbasse (дата обращения: 18.02.2024).

2. Военная спецоперация России: решения, которые спасают жизни [Электронный ресурс]. – Режим доступа: https://www.vesti.ru/article/2682605 (дата обращения: 18.02.2024).

3. Лапина И.Ю., Каргапольцев С.Ю. Военная история и патриотизм в системе социально-экономических и политических связей в прошлом и настоящем (постановка проблемы) // Вестник гражданских инженеров. – 2015. – № 5 (52). – С. 330-342.

4. Ляукина, Г.А., Ефимов, Е.Г. (2015). Формирование патриотизма студентов в социальных интернет-сетях, Казанский педагогический журнал, 6-2 (113), С. 347-351.

5. Солдатова, Г.У., Рассказова, Е.И., Чигарькова, С.В., Львова, Е.Н. (2018). Цифровая культура: правила, ответственность и регуляция. В Р.В. Ершова (ред.) Цифровое общество как культурно-исторический контекст развития человека. Сборник научных статей и материалов международной конференции, С. 374-379.

6. Шаповалова А.М., Вагина В.О. (2021). Развитие патриотизма в молодежной среде в онлайн-пространстве. Caucasian Science Bridge, 4 (3), С. 44-52. doi: https://doi.org/10.18522/2658-5820.2021.3.4.

AFONIN Andrey Alexandrovich
Senior Lecturer, Far Eastern Federal University, Russia, Vladivostok

PATRIOTISM AS A FACTOR IN THE POLITICAL LIFE OF MODERN RUSSIA ON THE EXAMPLE OF THE MEDIA SPACE

Abstract. *The article examines the topic of translational practices of patriotism in the political media space of modern Russia. The author explores the ways, means and mechanisms by which patriotic ideas and values are transmitted through various media channels and formats. Special attention is paid to the role of state and non-state actors in the process of forming and spreading patriotic sentiments among the population. The article examines various strategies and tactics of using media to strengthen national self-knowledge and increase civic engagement. The article analyzes the discourse of patriotism in the context of the influence of various conflict-causing factors in the development of the modern Russian political process and in order to study technologies for maintaining civil harmony in the context of ethno-political diversity. The complex problems of patriotism as a valuable phenomenon of the political life of society are being actualized. The author substantiates the procedural nature of the discursive construction of political reality, as well as the axiological content of discourse analysis as a method of political science. The article is devoted to the current problem of de-information in the political process. In the course of the research, the author comes to the conclusion that the most significant skill of a journalist is an objective assessment of events and phenomena.*

Keywords: *patriotism, media space, discourse, Internet, politics.*

ФИЛОСОФИЯ

ГОЛУБ Николай Николаевич
доцент кафедры управления, кандидат философских наук,
Московский государственный университет имени М. В. Ломоносова –
Севастопольский филиал, Россия, г. Севастополь

ЖУК Оксана Андреевна
студентка, Московский государственный университет имени М. В. Ломоносова –
Севастопольский филиал, Россия, г. Севастополь

КОНЦЕПЦИЯ ИДЕАЛЬНОГО ГОСУДАРСТВА В ФИЛОСОФИИ ПЛАТОНА

Аннотация. *В данной научной статье рассматривается решение проблемы совершенного устройства государства античным философом Платоном. Рассмотрены основные принципы построения «идеального государства», описаны методы разрешения конфликтов между гражданами, сословное устройство и функции каждого социального слоя, а также важные качества, которыми должен обладать правитель такого государства. Кроме того, в статье дан сравнительный анализ учений Платона, Аристотеля и Сократа, а также рассмотрена критика Карлом Поппером концепции Платона.*

Ключевые слова: *Платон, государство, философ, учение Платона, идеальное государство, справедливость, Карл Поппер, Аристотель, Сократ.*

Во все времена общество было озадачено поиском модели идеального государство. Перед современной философской российской наукой стоит задача разработки концепции совершенного государства, главной целью которого является обеспечение стабильной и благополучной жизни его граждан. Общество вновь и вновь возвращается к теме идеального государства, подразумевая демократическое и правовое государство. Поэтому тема исследования проблемы идеального государства актуальна всегда. В данной статье проводится сравнительный анализ концепций идеального государства в работах философов античности и выдвигаются принципы идеального государства в современных реалиях. Целью нашего исследования является составление сравнительного анализа концепций идеального государства различных философов. Методы исследования: сравнительно-описательный, исторический, а также методы анализа, синтеза.

Одной из наиболее знаменитых, обсуждаемых и одновременно критикуемых концепций в политической философии является концепция идеального государства Платона. Ряд философов считает ее несовместимой с потребностями социума и реальными условиями существования человека в мире, а потому нереалистичной и утопичной.

Модель государства Платона базируется на разделении власти, гармонии между гражданами и справедливости. Важнейший постулат, обеспечивающий существование идеального государства, состоит в том, что каждый член общества обязан выполнять только то дело, к которому он наиболее способен [6]. Все граждане должны жить в мире и согласии друг с другом, стремиться к общему благу и справедливости. Основными добродетелями в таком государстве считаются мудрость, мужество, рассудительность и справедливость [7].

Во-первых, государство Платона характеризует отсутствие частной собственности. По мысли античного философа, частная собственность в государстве порождает неравенство граждан и, соответственно, конфликты. В свою очередь, существующие разногласия в государстве должны разрешаться путем диалога и поиска истинного знания. При этом распределение государственного имущества должно происходить в соответствии с потребностями каждого члена социума [1].

Во-вторых, по Платону, большое внимание в «идеальном» государстве должно уделяться образованию и воспитанию гражданских ценностей.

В-третьих, для достижения благополучия всех людей, проживающих в государстве, необходимо четкое разделение обязанностей между членами общества [4].

Так, правят в таком государстве философы, обладающие знаниями и мудростью. Именно это «сословие» обуславливают благосостояние и справедливость, царящие в государстве Платона. Они оберегают «совершенный» строй, законы от «сомнительных» нововведений. Их деятельность обуславливает само существование идеального государства, его неизменность.

Важно отметить, что Платон разделяет общество на три класса: правители, стражи и производители. Переход из класса в класс возможен, но должен происходить под контролем правителя. Правители занимаются управлением государством, производители – производством и обеспечением материальных потребностей общества, а стражи обеспечивают безопасность и защиту [3]. При этом все производственные заботы ложатся на ремесленников и земледельцев. Философы, стоящие во главе государства, по Платону – высшие и самые рациональные члены общества. Они имеют отличное образование и глубокое понимание истины и справедливости. Античный философ полагал, что образование должно быть доступным для всех и направленным на совершенствование нравственных и умственных качеств людей. Правители на основах разума осуществляют управление более низкими по статусу «сословиями», ограничивая при этом их свободу.

Взгляды на идеальное государство можно встретить в трудах многих философов античности. Основателем философского учения о государстве считается древнегреческий философ Сократ. В своих беседах мудрец выделял пять форм правления: монархия (царство), тирания, плутократия, аристократия и демократия. Различия этих форм он видел в способах и целях существования власти. В «идеальном государстве», по представлениям Сократа, правят лучшие, царят разум и добродетель [5, с. 36-41]. То есть, Сократа, как и его ученика Платона, можно назвать идеалистом. Платон позаимствовал у своего учителя много идей об идеальном государстве, дополнил их и разработал концепции форм государства, которые, хотя и были в некотором смысле утопическими, для теории науки о государстве с исторической точки зрения считаются более развернутыми и завершенными.

Приемник Платона Аристотель совершенным государством считал «смешанное государство», которое имеет достоинства и демократии, и аристократии, и монархии. Аристотель исходил в своих суждениях из анализа описанных им форм государственного устройства полисов, их преимуществ и недостатков. По мнению Аристотеля, существовало три типа «правильных» форм правления в государстве: монархия, где власть передается правителю по наследству, аристократия, где властвуют лучшие, и демократия, где власть осуществляется гражданами государства. Данную форму государства он назвал «политией». «Полития» Аристотеля – это идеальное государство «золотой середины», в котором наблюдается умеренность во всем: и в количестве законов, и в размере территории. Этот мыслитель раскритиковал идеальное государство Платона и отстаивал важность частной собственности и необходимость семьи для государства. Согласно Аристотелю, источник общественного зла – не столько собственность, сколько бесконечность желаний человека и его алчность, которая направлена и на почести, поэтому «нужно более заботиться о том, чтобы уравнять желания граждан, нежели их имущества».

Соответственно, в мировоззрениях Аристотеля и его учителя Платона – много общего, однако есть и различия во мнениях, в частности, относительно форм государства, отношения к частной собственности.

Подход Платона к пониманию устройства государства некоторые философы истинным не считали. Одним из наиболее ярких критиков концепции «идеального» государства Платона считается представитель философии постпозитивизма Карл Поппер. В работе «Открытое общество и его враги», посвященной анализу древнегреческой демократии, исследователь выражает скептическое отношение к идее коллективизма в государстве: «Коллективизм, является преградой для развития индивидуальности, личность при этом бывает вынуждена подчинить свои личные интересы интересам коллектива». По мнению Карла Поппера, человек в условиях платоновского устройства государства не способен реализовать свой потенциал, что негативно влияет на каждого гражданина в отдельности [2].

По мысли австро-британского философа, государство Платона базируется «на тоталитарной форме правления». При этом низшие слои общества с самого рождения подчиняются «руководителям». Поэтому у «исполнителей» формируется образ мышления раба, не способного принимать решения и отстаивать свои права.

Идее государственного устройства Платона Карл Поппер противопоставляет демократическое общество, которое он характеризуется таким образом: равенство всех граждан перед законом, право каждого гражданина выбирать правительство и самому быть избранным в состав правительства, возможность заниматься деятельностью по своему выбору, защита прав граждан и частной собственности со стороны государства [2].

Кроме того, важнейшая гипотеза Карла Поппера, высказанная в произведении «Открытое общество и его враги», заключается в том, что государство Платона является закрытым, то есть в нем запрещен переход из одного сословия в другое. Австро-британский философ, в свою очередь, выдвигает гипотезу об открытом обществе, где межсословный переход возможен. По мысли Карла Поппера, именно в таком обществе соблюдается важнейший принцип социальной справедливости. На наш взгляд, идеальным государством является то государство, в котором максимально удовлетворяются интересы всех его граждан. Поскольку граждане страны являются высшей ценностью, носителем суверенитета и единственным источником власти. Главными принципами идеального государства являются равноправие и взаимоуважение всех граждан, независимо от пола, расы, национальности, языка и вероисповедания, справедливость и верховенство закона. Данная концепция позволит избежать социальной, расовой, национальной или религиозной вражды и ненависти, что в современном мире является залогом устойчивого развития любого государства.

Таким образом, вопрос о возможности и методах построения «идеального» государства остается актуальным и при этом нерешенным до конца по сей день. Важность учения Платона заключается в том, что оно положило начало теориям социального управления в наиболее широком смысле слова. Вместе с тем сейчас очевидны недостатки его учения. Прежде всего, нужно отметить, что невозможно доказать, что идея государства Платона нашла воплощение в реальности. Республика, созданная воображением античного философа, существует только в его сочинениях. Сам Платон утверждал, что его государство реализовано только в вечном мире форм и идей. Идеальное государство Платона есть не что иное, как чистая идея, метафора.

Литература

1. Жулёв Н.А. Экономика и право: монография / Н.А. Жулёв, А.Ю. Гребенников, В.В. Смирнов [и др.]. – Чебоксары: ИД «Среда», 2021. – 172 с. – ISBN 978-5-907411-11-1. – DOI 10.31483/a-10248.

2. Карл Поппер: Открытое общество и его враги. том 1. Чары Платона. Дополнение 3. ответ на критику (1961).

3. Каткова Я.А., Пятилетова Л.В. Уральский государственный университет путей сообщения. Концепция идеального государства Платона.

4. Клыкова М.А / Научно- издательский центр аспект. Учение об идеальном государстве Платона.

5. Кодзоков И.А. Формы государства и концепции «идеального государства» в учениях Сократа, Платона и Аристотеля // Вопросы российского и международного права. 2021. Том 11. № 10А. С. 36-41. DOI: 10.34670/AR.2021.31.54.004.

6. Поляков Е.Н., Крюкова Ю.Е.. Концепция «идеального» города-государства в трудах Платона (427–347 гг. до н. э.).

7. Тепляшин И.В., Лукашевский Д.С. / Журнал Право и государство: теория и практика. Учение Платона об идеальном государстве и его актуальность в современной правовой действительности.

GOLUB Nikolay Nikolaevich
Associate Professor of the Department of Management, Candidate of Philosophical Sciences,
Lomonosov Moscow State University – Sevastopol Branch, Russia, Sevastopol

ZHUK Oksana Andreevna
Student, Lomonosov Moscow State University – Sevastopol Branch,
Russia, Sevastopol

THE CONCEPT OF AN IDEAL STATE IN PLATO'S PHILOSOPHY

Abstract. *This scientific article examines the solution to the problem of the perfect organization of the state by the ancient philosopher Plato. The main principles of building an "ideal state" are considered, methods of resolving conflicts between citizens, the social structure and functions of each social class, as well as important qualities that a ruler of such a state should possess. In addition, the article provides a comparative analysis of the teachings of Plato, Aristotle, and Socrates, as well as criticism of Plato's concept by Karl Popper.*

Keywords: *Plato, state, philosopher, Plato's teaching, ideal state, justice, Karl Popper, Aristotle, Socrates.*

ЮРИСПРУДЕНЦИЯ

БЕЛОЗЕРСКИХ Даниил Сергеевич
аспирант, Белгородский университет кооперации, экономики и права,
Россия, г. Белгород

Научный руководитель – доцент кафедры гражданского права и процесса Белгородского университета кооперации, экономики и права, доцент Внукова Валентина Арсентьева

ДОКТРИНАЛЬНЫЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ДОГОВОРА СИНДИЦИРОВАННОГО КРЕДИТА

Аннотация. *Статья посвящена рассмотрению роли и значения теоретических подходов к определению конструкции синдицированного кредитования. Наиболее важную часть работы составляет описание и анализ дефиниции договора синдицированного кредита.*

Ключевые слова: *договор синдицированного кредита, кредит, синдикат, кредитор, заемщик, кредитный договор.*

Подходы к определению понятия «синдицированный кредит» разнообразны как в отечественной доктрине, так и в зарубежной. Термин «синдицированный кредит» (syndicated loan) берет начало из англо-саксонской правовой системы и обозначает совокупность автономных (параллельных) кредитов, предоставленных группой кредиторов одному заемщику на одинаковых условиях как для кредиторов, так и для заемщика. Для такой конструкции характерно одно соглашение между кредиторами и разветвленная сеть договоров между кредиторами и заемщиком.

В романо-германской система также существует институт совместного финансирования, предполагающий множественность на стороне кредитора – консорциальный кредит (konsortialdarlehensvertrag). Немецкая конструкция совместного финансирования предполагает совместное предоставление кредита за общий счет несколькими кредитными организациями в рамках договора простого товарищества. Для такой формы характерно заключение единого договора между кредиторами и заемщиком.

Институт синдицированного кредитования по российскому законодательству по содержанию тяготеет к английской договорной конструкции. В отечественной доктрине синдицированный кредит продолжительное время обозначался как разновидность кредита, при которой в сделке участвуют два и более банка. Характеристика института сводилась к активной множественности на стороне кредитора и общности документации. В последнее время изучение сместилось в плоскость правовых основ синдицированного кредитования, что представляет интерес в связи со сложной структурой сделки, включающей в себя совокупность гражданско-правовых договоров, которые опосредуют предоставление финансирования заемщику. Будет правильно отметить, что отечественная юридическая наука до сих пор воспринимает синдицированный кредит как новое явление. Унификации в определении таких понятий, как «синдицированный кредит», «синдицированное кредитование» со свойственной для данного института спецификой в доктрине не сложилось. Большинство российских исследователей квалифицируют синдицированный кредит в качестве одной из форм традиционного кредита. В частности, в литературе, отмечается, «что синдицированный кредит является разновидностью банковского кредита, основанного на базовых принципах банковского кредитования (принцип

срочности, платности, возвратности, в отдельных случаях, обеспеченности и целевого характера), отличительной особенностью которого является специфический механизм аккумуляции кредитных ресурсов и их предоставления заемщику» [2, с. 21]. Как отмечают другие авторы, анализирующие правовую природу синдицированного кредита – «это в первую очередь соглашение между кредиторами» [1, с. 8]. В работах Качаловой А. В. под синдицированным кредитом подразумевается такая разновидность кредита, «при которой в кредитной сделке принимают участие не менее двух банков, каждый из которых предоставляет определенную часть необходимой заемщику суммы кредита, используя при этом общие для всех участников синдицированного кредита формы договоров, а сам кредит управляется специальным агентом, функции которого могут быть возложены на один из банков-участников (банк-агент)» [3, с. 57]. Определение, которое дано Качаловой А. В., имеет ряд слабых сторон, например, в качестве субъектов, выступающих в роли кредитора, автором выделены исключительно банки, что существенно ограничивает круг лиц, которые могут выступать в данной роли и не отражает действительную ситуацию на финансовом рынке. А. И. Сапункова предлагает рассматривать синдицированный кредит как «разновидность заемного обязательства, по которому два или более кредиторов (синдикат кредиторов) обязуются предоставить одному заемщику денежные средства на условиях, определенных договором синдицированного кредита, а последний обязуется возвратить в установленный срок полученную денежную сумму, проценты за ее использование, а также возместить кредиторам иные расходы, связанные с предоставлением денежных средств» [6, с. 28]. Предложенное Сапунковой А. И. определение схоже с определением кредита, которое дано в ст. 819 Гражданского кодекса Российской Федерации (далее ГК РФ), хотя и отражает одну из специфик рассматриваемого института - множественность кредиторов. Указание на конкретный порядок возмещения расходов при организации сделки, представляется излишним ввиду того, что детальное урегулирование всех действий сторон, приводит к косности правоотношений, по мнению автора данные положения подлежат урегулированию сторонами в договоре. Рассмотрение синдицированного кредита в качестве особой стратегии, позволяющей кредиторам распределить риск неисполнения или ненадлежащего исполнения (кредитный риск), а заемщикам получить доступ к нескольким источникам финансирования, отражает исключительно экономическую составляющую института, не учитывая правовую. Как уже ранее отмечалось, первоначально, при зарождении синдицированного кредитования, основной фокус был на экономической составляющей института. В настоящее время изучение синдицированного кредитования исключительно через экономическую призму представляется недостаточным для разрешения возникающих проблем, в том числе при правоприменении.

В доктрине довольно широкое отражение нашло деление синдицированного кредита на виды в зависимости от того или иного критерия. К примеру, Рыкова И. Н. выделяет следующие виды: «совместно инициированный синдицированный кредит, индивидуально инициированный синдицированный кредит (формирует вторичный рынок кредитования посредством уступки), синдицированный кредит без определения долевых участий» [5, с. 11-22]. В зависимости от валюты кредита выделяют моновалютный (single-currency loan) и мультивалютный (multi-currency loan). Стоит отметить, что в отличие от традиционного кредита, синдицированный кредит может быть, как моновалютным, так и мультивалютным. В зависимости от кредитного качества заемщика можно выделить высококачественный (investment-grade loan) синдицированный кредит и рисковый (leveraged loan) синдицированный кредит. В зависимости от формы участия в доктрине различают участие в фондировании (funded sub-participation) и участие в риске (risk sub-participation), классическая синдикация (primary syndication/direct participation). Классическая синдикация встречается чаще всего на практике и подразумевает участие кредиторов на стадии заключения договора, для синдикации данного вида характерна особая процедура преддоговорного взаимодействия сторон и порядок заключения договора, включающая несколько этапов – предоставление мандата, структурирование и синдикацию, что прямо не урегулировано в российском законодательстве. К участию в первичной синдикации привлекается широкий круг кредиторов, что, к примеру, отличает ее от клубной сделки (club deal loans) (табл.).

Таблица

Сравнительная характеристика договора синдицированного кредита и клубного кредитного договора

Критерий сравнения	Договор синдицированного кредита	Клубный кредитный договор
Объем	Вовлечение в сделку широкого круга инвесторов дает возможность привлекать существенные объемы финансирования	Объем доступных средств ограничен лимитами партнеров.
Участники сделки	Широкий круг кредиторов	Кредиторы партнеры
Количество участников	Ограничений нет	До 5 кредиторов

В клубной сделке участвует небольшое число кредиторов (зачастую банки), как правило, уже имеющих взаимоотношения с заемщиком, а сама сделка имеет небольшой объем. «Под клубным кредитом понимается любой синдицированный кредит, не предполагающий рыночную синдикацию (retail/general syndication) и, как правило, предоставляемый ограниченным кругом инвесторов – основных обслуживающих банков заемщика (relationship banks)» [4, с. 17]. В рамках клубного кредита заемщик самостоятельно проводит синдикацию на рынке и привлекает кредиторов, с которыми у него установлены коммерческие взаимоотношения. Отечественный формат синдицированного кредита больше напоминает клубную сделку.

Литература

1. Гаген А. Синдицированный кредит. Перспективы развития синдицированного кредита в РФ // Информационное агентство «Финансовый юрист» [электронный ресурс]: http://www.financial-lawyer.ru/newsbox/kredit/139-528070.html (дата обращения 02.09.2022).

2. Григорьева О.М. Организация синдицированного кредитования в России. Дисс. на соиск. уч. ст. к.э.н. М., 2004.

3. Качалова, А.В. Правовые особенности заключения договоров о предоставлении синдицированных кредитов / А.В. Качалова // Законодательство. 2006. № 2. – С. 57.

4. Кукоба А. Рыночные синдикации vs клубные сделки: за и против // Справочник эмитента. 2011. URL: http://review.cbonds.info/article/references/217/ (дата обращения 27.04.2023).

5. Рыкова, И.Н. Рынок новых кредитных продуктов: проблемы и перспективы в России / И.Н. Рыкова // Финансы и кредит. – 2007. – № 32. – С. 11-22.

6. Сапункова, А.И. Правовое регулирование синдицированного кредитования в международном коммерческом обороте. Автореферат. Москва. 2008. – URL: https://www.alpmsu.ru/science/Sapunkova.pdf.

BELOZERSKIKH Daniil Sergeevich
Postgraduate student,
Belgorod University of Cooperation, Economics and Law, Russia, Belgorod

Scientific Advisor – Associate Professor of the Department of Civil Law and Procedure of the Belgorod University of Cooperation, Economics and Law, Associate Professor Vnukova Valentina Arsentieva

DOCTRINAL APPROACHES TO THE DEFINITION OF A SYNDICATED LOAN AGREEMENT

Abstract. *The article is devoted to the consideration of the role and significance of theoretical approaches to the definition of syndicated lending. The most important part of the paper is the description and analysis of the definition of the syndicated loan agreement.*

Keywords: *syndicated loan agreement, loan, syndicate, lender, borrower, loan agreement.*

СИДОРОВА Дарья Александровна
студентка магистратуры,
Московский финансово-юридический университет МФЮА, Россия, г. Москва

ПРОБЛЕМНЫЕ АСПЕКТЫ И ЗАКОНОДАТЕЛЬНЫЕ ОСНОВЫ ПРОЦЕДУРЫ АДМИНИСТРАТИВНЫХ СПОРОВ: АНАЛИЗ ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ

Аннотация. *В статье исследованы актуальные вопросы, связанные процедурой административных споров. Автором обозначены проблемные аспекты правоприменительной практики, а также законодательные основы процессуального обеспечения института административных споров.*

Ключевые слова: *административный спор, правовой спор, субъект, сторона, конфликт.*

Административные споры относятся к одним из самых распространенных в отечественной судебной практике. Обоснованно это прежде всего распространенностью самих административных правоотношений.

Во-первых, сущность любого спора требуется рассматривать через призму наличия взаимных претензий сторон друг к другу по поводу определенного объекта. Указанное характерно для споров, возникающих в частном порядке. Во-вторых, существо спора носит межотраслевой характер.

В-третьих, данного рода спор предполагает строго определенную процессуальную оболочку, что его позволяет разграничить со спорами и конфликтами, имеющими место быть в повседневной жизни человека.

По справедливому замечанию Н.В. Сухова и Г.М. Миннуллина основную группу участников судебного разбирательства составляют «субъекты, собирательно именуемые в законодательстве как «лица, участвующие в деле»: это стороны, третьи лица, прокурор, лица, обращающиеся в суд за защитой прав, свобод и законных интересов других лиц или вступающие в процесс для дачи заключения» [1].

Действующее законодательство по-разному именует стороны в административном деле: в КАС законодатель использует термины «административный истец» [2] и «административный ответчик», а согласно статье 40 АПК РФ – «заявители» и «заинтересованные лица».

В публично-правовом отношении, из которого вытекает административно-правовой спор, имеется, как правило, два вида участников [3]:

а) субъекты, представляющие публичный интерес, выполняющие публичные функции и наделенные публичными правами для их осуществления в виде властных полномочий;

б) лица, представляющие частный интерес. В этом правоотношении в качестве обязательного субъекта присутствует публичная сторона, а другой стороной, как правило, выступают представляющие свой интерес частные лица.

Всегда при административных спорах одной из сторон является тот или иной исполнительный орган (должностное лицо), чьи действия или решения служат предметом конкретного спора.

Специфику административных споров определяет само существо административных правоотношений, которое, в свою очередь, следует рассматривать через призму общественных отношений, возникающих в сфере государственного управления, урегулированные нормами административного права. Сущность общественных отношений данного рода не предполагает непосредственного существования спора, но и не исключает его.

Ввиду чего признаки, присущие административно-правовым отношениям, непосредственным образом определяют сущность административно-правовых споров.

Во-первых, административный спор отличается субъектным составом.

Во-вторых, как уже было отменно выше, неравенство субъектов имеет место быть в административных правоотношениях, но при возникновении административного спора участники равны перед судом и имеют равные процессуальные полномочия.

В-третьих, между сторонами имеется спор, сущность которого требуется рассматривать через призму расхождения правовых позиций по связывающему их спорному правоотношению.

Четвертый признак неразрывным образом связан с предыдущим ввиду того, что расхождение позиций связано с применением, нарушением, различным толкованием норм публичного права и реализацией определяемых ими субъективных публичных прав и обязанностей;

В качестве еще двух признаков, следует выделить специфику предмета спора, которым являются субъективные публичные права и законность административных актов, а также наличие определённой процедуры его заявления и разрешения.

Характерными признаками, свойственными административным спорам являются:

- специфический субъектный состав, обусловленный природой административно-правовых отношений, где одной стороной выступает орган публичной власти или должностное лицо.
- юридическое равенство участников административного спора,
- наличие разногласий между сторонами административного спора относительно одного и того же правоотношения,
- предметом спора вступают субъективные публичные права и законность административных актов,
- специфика процедуры административного спора.

Подводя итоги, следует отметить, что административно-правовой спор представляет собой разногласия между субъектами административно-правовых отношений различно понимаемых взаимных прав и обязанностей и (или) законности административных актов, возникающие в связи с реализацией, применением, нарушением либо установлением правовых норм в сфере публичного управления и разрешаемые в рамках определенной административной процедуры.

Литература

1. Сухова Н.В., Миннуллина Г.М. Проблема определения сторон в гражданском процессе // Вестник магистратуры. 2015. №1. С.76.

2. Ст.38 Кодекса административного судопроизводства Российской Федерации от 08.03.2015 N 21-ФЗ.

3. Административное дело и административно-правовой спор: понятие и соотношение А. В. Глодина, с.7 http://www.vestnik.vsu.ru/pdf/pravo/2017/03/2017-03-14.pdf

SIDOROVA Daria Alexandrovna
Graduate student,
Moscow University of Finance and Law, Russia, Moscow

PROBLEMATIC ASPECTS AND LEGISLATIVE BASES OF THE ADMINISTRATIVE DISPUTE PROCEDURE: ANALYSIS OF LAW ENFORCEMENT PRACTICE

Abstract. *The article examines topical issues related to the procedure of administrative disputes. The author identifies problematic aspects of law enforcement practice, as well as the legislative basis for the procedural support of the institute of administrative disputes.*

Keywords: *administrative dispute, legal dispute, subject, party, conflict.*

ФЕДОРОВ Данила Дмитриевич
магистрант, Тамбовский государственный университет им. Г. Р. Державина,
Россия, г. Тамбов

Научный руководитель – заведующий кафедрой уголовного права и процесса Тамбовского государственного университета им. Г. Р. Державина, кандидат юридических наук, доцент Попова Елена Альбертовна

АДМИНИСТРАТИВНЫЙ НАДЗОР КАК ИНСТРУМЕНТ ПРЕДУПРЕЖДЕНИЯ РЕЦИДИВА ПРЕСТУПЛЕНИЙ

Аннотация. *В статье рассматривается механизм административного надзора как принудительного правового средства предупреждения рецидива преступлений. Обращено внимание на исторически сложившуюся действенность данного инструмента предупреждения рецидива. Установлены задачи, виды и основания административных ограничений в отношении поднадзорных лиц.*

Ключевые слова: *административный надзор, административное ограничение, органы внутренних дел, поднадзорное лицо, рецидив преступлений.*

Профилактика рецидивной преступности является важной социальной задачей, которую государство всегда определяло в числе приоритетных. Это обусловлено высокой степенью общественной опасности рецидивистов, устойчивости данного поведения, а в ряде случаев преступные действия носят профессиональную направленность.

Одной из реально работающих мер профилактики рецидивной преступности можно назвать административный надзор.

Впервые институт административного надзора появился в СССР в 1966 году и был закреплен Указом Президиума ВС СССР от 26.07.1966 года № 5364-VI «Об административном надзоре органов внутренних дел за лицами, освобожденными из мест лишения свободы». Данный Указ утверждал Положение об административном надзоре органов внутренних дел за лицами, освобожденными из мест лишения свободы, которое действовало в различных редакциях вплоть до 01.01.2010 года.

Важно подчеркнуть, что в первоначальной редакции мероприятия административного надзора, в первую очередь, были направлены на особо опасных рецидивистов. Далее круг лиц, подпадающих под административный надзор, только расширялся – так, например, была добавлена категория судимых два и более раза к лишению свободы за любые умышленные преступления. В ходе внесения изменений в нормативные акты указанной тематики изменялись и сроки административного надзора – от шести месяцев до года, в случае необходимости предусматривалось продление каждый раз еще на шесть месяцев, но не свыше сроков, предусмотренных законом для погашения или снятия судимости за данное преступление.

Первоначально обязанность по установлению административного надзора вменялась милиции (по месту жительства), однако в сентябре 1983 года были внесены изменения в порядок надзора за особо опасными рецидивистами, а также лицами, чье «поведение в период отбывания наказания в местах лишения свободы свидетельствует об упорном нежелании встать на путь исправления и приобщения к честной трудовой жизни» [6]. Теперь данная обязанность закреплялась за руководством исправительного учреждения (при освобождении), путем вынесения мотивированного постановления, с указанием оснований, сроков административного надзора.

Это в очередной раз подчеркивает важность в советском законодательстве института административного надзора в деле профилактики повторной преступности.

Результаты исследований того времени (более чем за десятилетний период) показывают, что в 20% случаев поднадзорные привлекались к уголовной ответственности за злостное нарушение правил административного надзора (причем, в основном, осуждались к уголовным

наказаниям, не связанным с лишением свободы) и лишь 10% – за совершение иных преступлений. Учитывая стойкую антиобщественную установку личности поднадзорных, это небольшая цифра [1, с. 41].

Конец XX века ознаменован как ростом преступности, с одной стороны, так и практически полным отмиранием советского законодательства, регламентирующего в том числе систему предупреждения повторных преступных деяний. Так, в принятом в 1991 году Законе Российской Федерации «О милиции», положения, касаемые административного надзора, полностью отсутствуют. Справедливости ради надо отметить, что Положение об административном надзоре в редакции от 1983 года действовало вплоть до 01.01.2010 года, однако действие это было юридически формальным.

Именно поэтому важное значение имело принятие федерального закона от 06.04.2011 года № 64-ФЗ «Об административном надзоре за лицами, освобожденными из мест лишения свободы», восстановившего данный институт.

Указанный нормативный акт определяет административный надзор как осуществляемое органами внутренних дел наблюдение за соблюдением лицом, освобожденным из мест лишения свободы, установленных судом временных ограничений его прав и свобод, а также за выполнением им определенных обязанностей [7].

Главная цель – предупреждение преступлений и иных правонарушений, в том числе совершенных рецидивистами, путем осуществления индивидуальной профилактической работы с лицами, освобожденными из мест лишения свободы, а также наблюдения за указанным контингентом.

Необходимо отметить, что рецидив, в том числе опасный и особо опасный, существенно влияет на длительность сроков административного надзора: при простом рецидиве – от года до трех лет, опасном и особо опасном – на установленный срок для погашения судимости.

Криминологическим основанием применения административного надзора следует признать неблагоприятный прогноз индивидуального преступного поведения освобождающегося лица, но без конкретизации места, времени и способов совершения преступления. Это определяет профилактическую сущность данной меры как уголовно-правовой «меры безопасности» [8, с. 55].

В целях обеспечения профилактической составляющей положения федерального закона от 06.04.2011 года № 64-ФЗ «Об административном надзоре за лицами, освобожденными из мест лишения свободы» в отношении поднадзорного лица предусматривают определенные административные ограничения, то есть установленные судом временные ограничения прав и свобод.

Одни ограничения носят обязательный характер, другие – лишь могут устанавливаться при административном надзоре.

К обязательным относят запрет на выезд за установленные судом пределы территории лицам, не имеющим места жительства или пребывания; а также лицам, имеющим непогашенную либо неснятую судимость за совершение преступления против половой неприкосновенности и половой свободы несовершеннолетнего. Обязательна также явка поднадзорного лица от одного до четырех раз в месяц в орган внутренних дел по месту жительства, пребывания или фактического нахождения для регистрации [7].

Данная обязанность (явка от одного до четырех раз в месяц) в большей степени по сравнению с другими ограничениями позволяет сотрудникам органов внутренних дел непосредственно контролировать поднадзорное лицо.

Поскольку регулярное посещение территориального органа внутренних дел оказывает дисциплинирующее воздействие на осужденного, напоминает ему о необходимости соблюдения предусмотренных законодательством обязанностей и ограничений, недопущении совершения преступлений и иных правонарушений [2, с. 102].

Также отметим, что нельзя рассматривать административное ограничение как наказание, поскольку эта мера направлена на недопущение повторного преступления и является лишь одним из элементов административного надзора.

С точки зрения предупреждения рецидива преступлений цель административных ограничений – не допустить продолжения преступного поведения, пресечь появление новых преступных контактов и связей, исключить возможность совершения противоправных деяний с учетом определенного места и времени.

В соответствии с приказом МВД России от 08.07.2011 года № 818 «О Порядке осуществления административного надзора за лицами, освобожденными из мест лишения свободы»

обязанности в рамках административного надзора возложены на сотрудников различных структурных подразделений органов внутренних дел.

Функция профилактики преступлений в деятельность служб органов внутренних дел реализуется по-разному. Для некоторых служб данный вид деятельности является основным, для других – одним из основных, для третьих – является дополнением и реализуется в рамках проведения отдельных профилактических мероприятий (например, ночные рейды у сотрудников ДПС) [5, с. 235]

Основная же нагрузка по осуществлению профилактической работы в рамках административного надзора приходится на службу участковых уполномоченных полиции.

Работа данного подразделения полиции в рамках исполнения обязанностей по административному надзору строится по трем основным направлениям:

1. Непосредственное взаимодействие с поднадзорным лицом;
2. Обеспечение взаимодействия с другими субъектами административного надзора;
3. Документальное оформление результатов работы по указанному направлению.

Так, к первому направлению можно отнести наблюдение и посещение поднадзорных по месту жительства (не реже одного раза в месяц) в определенное время суток, в течение которого этим лицам запрещено пребывание вне указанных помещений, проведение с ними профилактических бесед [3].

Второе направление, как правило, обеспечивает обмен информацией как между службой участковых уполномоченных и иных подразделений полиции (оперативными дежурными, сотрудниками патрульно-постовой службы и др.), так и сотрудниками других ведомств (исправительных учреждений, мест работы поднадзорных).

Третье направление – оформление результатов профилактической работы (актирование посещения поднадзорного лица, заполнение маршрутного листа о поведении поднадзорного лица, подача рапорта на имя руководителя, ответственного за данное направление работы, о фактах нарушения административных ограничений, внесение информации в ведомственные информационные сервисы).

Вместе с тем, как справедливо отмечают некоторые авторы, механизм индивидуальной профилактической работы, проводимой органами внутренних дел с поднадзорным лицом, к сожалению, не в полной мере регламентируется ведомственными нормативными актами. Необходимый «набор» мер воздействия по предотвращению повторных преступлений должен быть тщательно проанализирован и выбран в зависимости от причин и условий, способствующих противоправному поведению поднадзорного лица [4, с. 64].

Для этого необходимо не только четкое взаимодействие структурных подразделений внутри территориального органа внутренних дел, но и совместная слаженная работа исправительных учреждений, полиции, трудовых коллективов.

Таким образом, административный надзор – важный элемент всей системы предупреждения преступности, в том числе и рецидивной. Его профилактическая составляющая заключается не только в воздействии и ограничениях, установленных для лиц, освобожденных из мест лишения свободы, но и в опосредованном влиянии на граждан, контактирующих с данной категорией лиц.

Литература

1. Векленко, В.В., Бекетов, О.И. Административный надзор милиции за лицами, освобожденными из мест лишения свободы: Аргументы в пользу восстановления // Полицейское право. 2006. № 1 (5). С. 38-42. – URL: https://www.elibrary.ru/download/elibrary_20220383_76174447.pdf (дата обращения 10.03.2024).
2. Возжанникова, И.Г. Рецидив как вид множественности преступлений: монография / отв. ред. А.И. Чучаев. М.: КОНТРАКТ, 2014. 112 с.
3. Приказ МВД России от 08.07.2011 № 818 «О Порядке осуществления административного надзора за лицами, освобожденными из мест лишения свободы» // Российская газета. 26.08.2011. № 189. СПС КонсультантПлюс.
4. Репьев, А.Г., Кашкина, Е.В. Специальные принципы осуществления административного надзора за лицами, освобожденными из мест лишения свободы: сущность, содержание и виды // Административное право и процесс. 2019. № 2. С. 61-65.
5. Савраскин, С.Н. Предупреждение рецидивной преступности лицами, состоящими под административным надзором // Научный журнал «Эпомен». 2022. № 28. С. 227-241. – URL: https://www.elibrary.ru/download/elibrary_

49408967_15433785.pdf (дата обращения 10.03.2024).

6. Указ Президиума ВС СССР от 26.07.1966 № 5364-VI «Об административном надзоре органов внутренних дел за лицами, освобожденными из мест лишения свободы» (ред. от 22.09.1983) // Ведомости ВС СССР. 27.07.1966. № 30. Ст. 597. СПС КонсультантПлюс.

7. Федеральный закон от 06.04.2011 № 64-ФЗ «Об административном надзоре за лицами, освобожденными из мест лишения свободы» // Собрание законодательства РФ. 11.04.2011. № 15. Ст. 2037. СПС КонсультантПлюс.

8. Фильченко, А.П. Административный надзор за лицами, освобожденными из мест лишения свободы: правовая природа и перспективы законодательного регулирования // Административное право и процесс. 2012. № 2. С. 54-57.

FEDOROV Danila Dmitrievich
master student, Tambov State University G. R. Derzhavin, Russia, Tambov

Scientific Advisor – Head of the Department of Criminal Law and Procedure at Tambov State University. G. R. Derzhavina, Candidate of Legal Sciences, Associate Professor Popova Elena Albertovna

ADMINISTRATIVE SUPERVISION AS A TOOL FOR PREVENTING THE RECURRENCE OF CRIMES

Abstract. *The article considers the mechanism of administrative supervision as a compulsory legal means of preventing the recurrence of crimes. Attention is drawn to the historically established effectiveness of this tool for preventing relapse. The tasks, types and grounds of administrative restrictions in relation to supervised persons have been established.*

Keywords: *administrative supervision, administrative restriction, police, supervised person, recidivism of crimes.*

ЯГНИКОВ Александр Андреевич
магистрант, Российский технологический университет МИРЭА,
Россия, г. Москва

Научный руководитель – доцент кафедры прикладного права Российского технологического университета МИРЭА, канд. юрид. наук, доцент Забайкалов Андрей Павлович

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИИ В СФЕРЕ ЭКОНОМИКИ

Аннотация. *В настоящей научной статье автор рассматривает особенности правового регулирования информации в сфере экономики. Для этого автор выделяет наиболее актуальные на практике направления экономической деятельности, где широко применяется разного рода информация. Далее автор кратко анализирует ключевые источники регулирования по каждому из обозначенных направлений. В заключении сделан вывод о перспективах развития действующего сегодня правового регулирования информации в сфере экономики.*

Ключевые слова: *развитие права, правовое регулирование информации, регулирование информации в сфере экономики, цифровизация, цифровая трансформация права.*

В сфере экономической деятельности информация является довольно актуальным и практически важным элементом, распространенным в самых разных категориях правоотношений. С цифровизацией экономики значимость информации существенно повысилась, поскольку возник большой объем качественно новых направлений экономической деятельности, реализуемой с использованием информационных технологий [3, с. 39-41]. В связи с этим вопрос о правовом регулировании такой информации становится все более актуальным.

Рассмотрим некоторые из наиболее востребованных направлений экономической деятельности, где информация выступает важной составляющей.

Прежде всего, необходимо говорить о защите данных. Экономика характеризуется различными типами взаимодействия, совершением сделок, в т. ч. международных и в сети Интернет, а потому вопрос о защите информации сегодня актуален, как никогда. Ключевым источником регулирования в данном случае выступает Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [8], который, собственно, является главным источником правового регулирования статуса информации не только в экономике, но и в любых других сферах и областях, где она в том или ином виде используется. Документ устанавливает правовые основы существования информации, определяет особенности ее сбора, хранения, передачи, закрепляет функции уполномоченных органов государственной власти в рассматриваемой сфере, а также субъектный состав правоотношений и т. д. В контексте защиты информации на международном уровне можно обозначить значительный ряд источников законодательства Европейского Союза, а также двусторонние договоры и соглашения.

Например, это профильные Регламенты и Директивы, посвященные защите персональных данных как таковых – с практической точки зрения крайне важная составляющая, которая в РФ приобрела высокую значимость относительно недавно, с принятием Федерального закона № 152-ФЗ «О персональных данных». На международном уровне примером такого документа выступает, в частности, Регламент ЕП и Совета ЕС № 2016/679 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных [1; 4]. Персональные данные относятся исключительно к физическим лицам, но для экономики выступают также значимой категорией, поскольку физические лица в полной мере являются участниками различных экономических отношений.

Здесь же в контексте рассмотрения вопроса о защите информации приведем еще несколько актуальных источников: например,

это Федеральный закон № 98-ФЗ «О коммерческой тайне», Указ Президента РФ № 188 «Об утверждении Перечня сведений конфиденциального характера», а также ряд других актов.

Второе направление – это антимонопольное законодательство, которое имеет целью своего регулирования защиту конкуренции и участников конкурентного рынка, предотвращение монополистической деятельности как таковой и т. д. Собственно, защите информации в Федеральном законе № 136-ФЗ «О защите конкуренции» посвящена глава 2.1, регламентирующая особенности защиты от недобросовестной конкуренции. Таковым может быть, например, распространение о конкуренте заведомо ложной информации, порочащей его деловую репутацию. Рассматриваемый нормативно-правовой акт определяет, каким образом подлежат привлечению к ответственности виновные в недобросовестной конкуренции субъекты правоотношений.

Особенности установления правового статуса информации требуются и в еще одной широкой и практически востребованной области – это права потребителей. Основным источником здесь Закон РФ № 2300-1 «О защите прав потребителей». В этом документе целый ряд статей посвящен регулированию использования информации в сфере защиты прав потребителей. Например, это касается нормативно установленного права каждого потребителя на информацию о товарах, работах или услугах. Законом, в частности, регламентирована сущность такой информации, ее правовые характеристики, а также установлена юридическая ответственность за несоблюдение указанных требований. Аналогичные положения закреплены, например, в отношении информации об изготовителе, продавце и т. д.

В отличие от представленных выше направлений, защита прав потребителей – актуальное направление в современной судебной практике [7, с. 130-133]. Это происходит, с одной стороны, из-за широкого практического распространения правоотношений данной категории, с другой – из-за значительного объема различных нарушений, допускаемых участниками сделок.

Обозначим еще одно актуальное направление, кратко уже упомянутое выше – это электронная коммерция, а также возникающие в этой связи отношения в области обеспечения кибербезопасности. Данное направление появилось в РФ не так давно, но уже приобрело высокую практическую значимость, а потому получило и соответствующее нормативное регламентирование. Перечислим некоторые источники, регулирующие правоотношения данной категории:

- Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»;
- Указ Президента РФ № 646 «Об утверждении Доктрины информационной безопасности РФ»;
- Указ Президента РФ № 260 «О некоторых вопросах информационной безопасности РФ»;
- КоАП РФ (ст. 13.12, посвященная административной ответственности за нарушение правил защиты информации);
- иные [5, с. 430-445; 9].

В данном направлении сегодня принято немало правовых источников, однако обеспечение защиты информации в сети Интернет продолжает оставаться актуальным, поскольку информационные технологии развиваются с более высокой скоростью, чем соответствующее правовое регулирование, возникают все новые составы правонарушений и преступлений в этой сфере. А то, что отношения имеют экономический характер, несет в себе еще и существенные материальные потери, которые зачастую имеют невосполнимый характер из-за того, что правоохранительные органы сталкиваются со значительными сложностями в расследовании киберпреступлений [10, с. 69-76]. Поэтому обеспечение кибербезопасности сегодня – важное и актуальное направление, нуждающееся в уделение особого внимания со стороны законодателя.

Кратко перечислим также некоторые иные направления экономической деятельности, где информация имеет наиболее значимый характер, и обозначим также ряд источников правового регулирования:

- подготовка финансовой отчетности, электронный документооборот (Федеральный закон № 402-ФЗ «О бухгалтерском учете», ст. 13, 18, 21 и другие, Федеральный закон № 63-ФЗ «Об электронной цифровой подписи, иные акты);
- защита информации как объекта интеллектуальной собственности (часть 4

Гражданского кодекса РФ, указанный выше Федеральный закон № 149-ФЗ, иные);

- иные.

Подведем итог изложенному выше вопросу.

Прежде всего, необходимо говорить о том, что информация сегодня распространена практически на все категории правоотношений в области осуществления экономической деятельности, а потому выступает значимым ее элементом.

Наиболее актуальный вопрос здесь – это, собственно, обеспечение защиты информации, ведь она касается и характеристик субъектного состава экономических отношений, и непосредственно содержания, и ряда других аспектов. С повсеместным распространением информационных технологий и внедрением в экономику процессов цифровизации тема защиты информации более актуализировалась, сегодня это буквально ключевое направление работы с ней.

В тексте научной статьи приведены отдельные направления экономической деятельности, в каждом из которых так или иначе используется информация, а также кратко проанализированы основные источники регулирования данных правоотношений. Можно обобщить, что существует ключевой нормативно-правовой акт, регламентирующий рассматриваемую сферу, – это Федеральный закон, определяющий особенности правового статуса информации, разного рода информационных технологий и защиты информации [8]. Также присутствует совокупность более профильных источников регулирования.

Тем не менее в настоящее время правовое регулирование информации в сфере экономики продолжает оставаться актуальным для совершенствования. В частности, это касается обеспечения защиты информации и в большей степени связано с акцентированием внимания на кибербезопасности.

Литература

1. Агасофия информации [Текст]: Коммуникативная концепция информации. Информационная модель мира: монография / Г.А. Атаманов; Федер. гос. авт. образоват. учреждение высш. образования «Волгогр. гос. ун-т». – Волгоград: Изд-во ВолГУ, 2017. – 122 с.

2. Акмаров, П.Б., Газетдинов, М.Х., Третьякова, Е.С. Проблемы защиты коммерческой информации в условиях цифровизации экономики // Вестник Казанского ГАУ. – 2020. – № 2 (58). – С. 133-139.

3. Борисов М.А. Проблемы правового регулирования информации в современных условиях // Конституционное и муниципальное право. – 2023. – № 6. – С. 39-41.

4. Лаптев, К.А. Обоснование необходимости правового и экономического регулирования информационных отношений в информационном обществе / К.А. Лаптев // Вестник евразийской науки. – 2021. – Т. 13. – № 5. – URL: https://esj.today/PDF/49ECVN521.pdf.

5. Мирских, И.Ю., Мингалева, Ж.А. К вопросу о правовом регулировании информации в условиях информационной экономики // Вестник Пермского университета. Юридические науки. – 2017. – № 38. – С. 430-445.

6. Палехова, Е.А. Понятие информации и цифровой экономики: правовые аспекты // Право и бизнес. – 2019. – № 2. – С. 46-49.

7. Петровская, О.В. Цифровая трансформация и проблемы обеспечения достоверности информации // Аграрное и земельное право. – 2020. – № 11. – С. 130-133.

8. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации». Российская газета. № 165. 29.07.2006.

9. Феткулин, Р.Р., Арюков, А.К. Преступления в сфере цифровой информации: понятие и виды // Baikal Research Journal. – 2019. – № 3. – Т. 10.

10. Чердаков О.И. Российское законодательство, обеспечивающее развитие отраслей, использующих информационные и цифровые технологии // Банковское право. – 2023. – № 4. – С. 69-76.

YAGNIKOV Alexander Andreevich
Graduate student, Russian Technological University MIREA,
Russia, Moscow

Scientific Advisor – Associate Professor of the Department of Applied Law of the Russian Technological University MIREA, Candidate of Law, Associate Professor Zabaikalov Andrey Pavlovich

LEGAL REGULATION OF INFORMATION IN THE FIELD OF ECONOMY

Abstract. *In this scientific article, the author examines the features of the legal regulation of information in the economic sphere. To do this, the author identifies the most relevant areas of economic activity in practice, where various types of information are widely used. Next, the author briefly analyzes the key sources of regulation for each of the identified areas. In conclusion, a conclusion is drawn about the prospects for the development of the current legal regulation of information in the economic sphere.*

Keywords: *development of law, legal regulation of information, regulation of information in the economic sphere, digitalization, digital transformation of law.*

Актуальные исследования

Международный научный журнал
2024 • № 11 (193)
Часть I

ISSN 2713-1513

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

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

Отпечатано в ООО «ЭПИЦЕНТР».
Номер подписан в печать 19.03.2024г. Формат 60×90/8. Тираж 500 экз. Цена свободная.
308010, г. Белгород, пр-т Б. Хмельницкого, 135, офис 40