АКТУАЛЬНЫЕ ИССЛЕДОВАНИЯ

МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ

ISSN 2713-1513

#20 (255), 2025

часть I

Актуальные исследования

Международный научный журнал
2025 • № 20 (255)
Часть I

Издается с ноября 2019 года Выходит еженедельно

ISSN 2713-1513

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

СОДЕРЖАНИЕ

МАТЕМАТИКА

ТЕХНИЧЕСКИЕ НАУКИ

ВОЕННОЕ ДЕЛО

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

АРХИТЕКТУРА, СТРОИТЕЛЬСТВО

НЕФТЯНАЯ ПРОМЫШЛЕННОСТЬ

МАТЕМАТИКА

МУСАБАЕВ Диас Зейноллаевич
магистрант,
Павлодарский государственный университет имени С. Торайгырова,
Республика Казахстан, г. Павлодар

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БИНАРНЫХ ОТНОШЕНИЙ ОБЪЕКТОВ КОНЕЧНЫХ ГРУПП

Аннотация. *Математическая аналитика таблиц Келли для 6 и 8 порядка конечных групп.*

Ключевые слова: *математика, конечные группы, таблицы.*

Построение таблицы Келли для группы шестого порядка

Построение таблиц Келли является важным инструментом визуализации структуры конечной группы и наглядной демонстрации её операций. Таблица Келли позволяет проследить, как элементы группы взаимодействуют между собой при бинарной операции, определённой на множестве.

Особый интерес представляют группы малого порядка, такие как группы порядка 6 и 8, поскольку они являются первыми примерами, где проявляются как абелевы, так и неабелевы структуры. Группа шестого порядка становится первым случаем появления неперестановочной (неабелевой) группы, а среди групп восьмого порядка уже существует значительное разнообразие: от полностью коммутативных до более сложных, таких как диэдральные и кватернионные группы.

В данном разделе будет подробно рассмотрено построение таблицы Келли для группы порядка 6. Такой подход не только способствует более глубокому пониманию абстрактных алгебраических структур, но и служит основой для алгоритмической реализации генерации таблиц в разрабатываемом программном обеспечении.

Существует два типа групп порядка 6 (до изоморфизма):

- циклическая группа C_6 – абелева группа, состоящая из 6 элементов;
- диэдральная группа D_3 – неабелева группа, представляющая симметрии равностороннего треугольника.

Особый интерес для исследования представляет диэдральная группа D_3, в дальнейшем будем именовать ее S_3. Она является простейшей неабелевой группой, в которой уже нарушается коммутативность операций. Поэтому именно она будет рассмотрена более подробно.

Группа $S_3 = \{e, a, a2, b, ab, a2b\}$ описывает все симметрии равностороннего треугольника: три поворота и три отражения. Состоит из следующих элементов:

- e – тождественное преобразование (нулевой поворот);
- a – поворот на 120° по часовой стрелке;
- a^2 – поворот на 240°;
- b – отражение относительно оси, проходящей через вершину и противоположную сторону;
- ab, ab^2 – отражения относительно других осей (рис. 1).

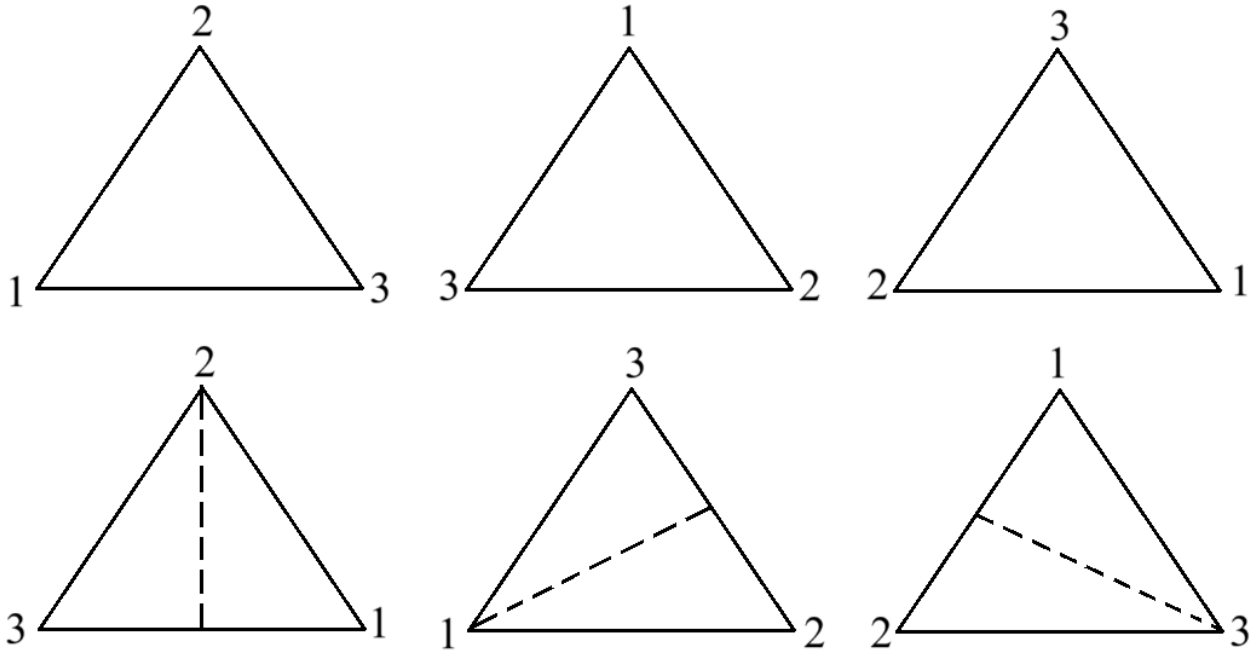

Рис. 1. Группа поворотов правильного треугольника

Генетический код группы $a^3 = e$, $b^2 = e$, $b \cdot a = a^2b$. Эта группа неабелева. Построим таблицу Келли группы S_3 (табл. 1).

Таблица 1

Таблица Келли группы S_3

	e	a^2	a	b	ab	a^2b
e	e	a^2	a	b	ab	a^2b
a	a	e	a^2	ab	a^2b	b
a^2	a^2	a	e	a^2b	b	ab
b	b	ab	a^2b	e	a^2	a
ab	ab	a^2b	b	a	e	a^2
a^2b	a^2b	b	ab	a^2	a	e

Построение таблицы Келли для группы восьмого порядка

Среди всех групп восьмого порядка особое место занимает диэдральная группа G_8 – группа симметрий квадрата, включающая повороты и осевые отражения. Эта группа является классическим примером неабелевой конечной группы, в которой бинарная операция (композиция преобразований) не удовлетворяет коммутативности.

Диэдральная группа порядка 8 состоит из восьми элементов: четырёх поворотов (включая тождественное преобразование) и четырёх отражений. Изучение её структуры важно как с теоретической, так и с практической точки зрения, поскольку такие группы естественным образом возникают в задачах, связанных с симметрией, геометрией, физикой и криптографией.

Таблица Келли, построенная для G_8, позволяет наглядно увидеть структуру группы: как выполняется ассоциативность, как различаются элементы по свойству обратимости, как взаимодействуют отражения с поворотами, и как именно проявляется некоммутативность операций. В данном подразделе будет пошагово рассмотрено построение таблицы Келли для G_8 с пояснениями к каждому действию и описанием полученного результата.

Элементы группы G_8 можно представить следующим образом:

- e – тождественное преобразование (нулевой поворот);
- a – поворот на 90° по часовой стрелке;
- a^2 – поворот на 180°;
- a^3 – поворот на 270°;

- b – отражение относительно вертикальной оси (проходит через середины противоположных сторон);
- ab – отражение относительно диагонали;
- a^2b – отражение относительно горизонтальной оси;
- a^3b – отражение относительно другой диагонали (рис. 2).

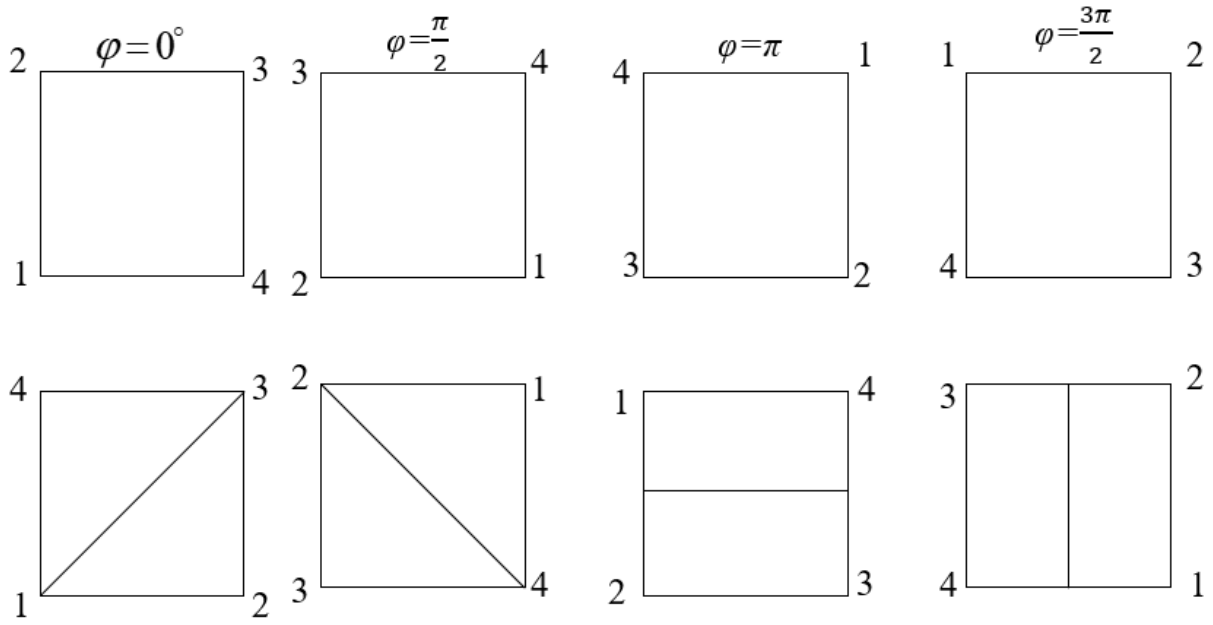

Рис. 2. Глядя на изложенные данные, можно получить элементы группы диэдра

$$\begin{aligned} 0°&: \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = a_1 \ \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix} = a_5 \\ \frac{\pi}{2}&: \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = a_2 \ \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} = a_6 \\ \pi&: \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = a_3 \ \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = a_7 \\ \frac{3\pi}{2}&: \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = a_4 \ \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = a_8 \end{aligned} \quad (1)$$

Таким образом, элементы диэдральной группы восьмого порядка можно записать в следующем виде $e = a_1; a = a_2; a^2 = a_3; a^3 = a_4; b = a_5; ab = a_8; a^2b = a_6; a^3b = a_7$.

Конечный вид группы диэдра восьмого порядка: $G_8 = \{e, a, a^2, a^3, b, a^2b, a^3b, ab\}$ с генетическим кодом $a^4 = e; b^2 = e; ba = a^3b$.

Таблица 2

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

MUSABAEV Dias Zeynollaevich
Master's student, S. Toraigyrov Pavlodar State University,
Republic of Kazakhstan, Pavlodar

SOFTWARE FOR BINARY RELATIONS OF FINITE GROUP OBJECTS

Abstract. *Mathematical analysis of Kelly tables for the 6th and 8th order of finite groups.*

Keywords: *mathematics, finite groups, tables.*

ТЕХНИЧЕСКИЕ НАУКИ

ИРЖАНОВ Арман
инженер по электрическим и телекоммуникационным системам,
ТОО «АНТИ КРАЖА», Республика Казахстан, г. Алматы

ИННОВАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ПЕРИМЕТРА С ПРИМЕНЕНИЕМ АКУСТОМАГНИТНЫХ СИСТЕМ И ИНТЕЛЛЕКТУАЛЬНОЙ ФИЛЬТРАЦИИ СИГНАЛОВ

Аннотация. *В статье рассматриваются современные подходы к повышению точности и надёжности работы акустомагнитных (АМ) охранных систем за счёт применения интеллектуальных методов фильтрации сигнала. Проанализированы типы помех, вызывающих ложные срабатывания, а также структурные и эксплуатационные особенности АМ-систем. Описаны методы спектрального, фазового, временного анализа и адаптивной фильтрации, направленные на повышение устойчивости системы к внешним воздействиям. Предложенные решения позволяют снизить количество ложных тревог, повысить селективность детекции и адаптировать системы под сложные условия эксплуатации.*

Ключевые слова: *акустомагнитная система, охрана периметра, ложные срабатывания, фильтрация сигнала, электромагнитные помехи, интеллектуальные алгоритмы, адаптивная обработка.*

Введение

Современные охранные системы играют ключевую роль в обеспечении безопасности объектов различного назначения – от розничных торговых площадей до складской и промышленной инфраструктуры. В условиях растущих угроз, связанных с хищениями, несанкционированным доступом и нарушением периметра, возрастает потребность в надёжных и точных системах обнаружения. Одним из широко используемых технических решений являются акустомагнитные (АМ) системы, отличающиеся высокой устойчивостью к внешним воздействиям, надёжностью и совместимостью с различными форматами защитных меток.

Несмотря на широкое распространение, АМ-системы подвержены ряду эксплуатационных проблем, в числе которых – ложные срабатывания, снижение чувствительности при электромагнитных помехах, деградация сигнала при нарушении калибровки и ошибки при установке оборудования. Эти проблемы снижают эффективность периметральной защиты, увеличивают затраты на обслуживание и создают дискомфорт для персонала и посетителей объектов.

Одним из перспективных направлений повышения надёжности АМ-систем является внедрение интеллектуальных методов фильтрации сигналов. В отличие от традиционного порогового срабатывания, такие методы предполагают анализ частотных, фазовых и временных характеристик сигнала, позволяя отличать помехи от подлинных тревожных событий. Использование адаптивных алгоритмов, временных фильтров и шаблонного сопоставления данных открывает возможности для создания более устойчивых и точных систем охраны.

Цель данной статьи – представить обзор и обоснование инновационных методов фильтрации сигналов в акустомагнитных системах защиты периметра, направленных на снижение числа ложных срабатываний и повышение точности обнаружения.

Принцип работы акустомагнитных систем

Акустомагнитные (АМ) системы относятся к числу наиболее надёжных технологий радиочастотной идентификации и периметральной охраны, широко применяемых в ритейле, логистике и учреждениях с высоким уровнем безопасности. Их работа основана на явлении

магнитострикции – изменении физических свойств материала под действием переменного магнитного поля, что позволяет фиксировать присутствие определённого резонансного объекта (метки) в зоне действия антенн.

Основной элемент системы – это антенны, выполняющие функции передатчика и приёмника сигнала. Передатчик создаёт мощное переменное магнитное поле с частотой около 58 кГц (в зависимости от производителя и модели), которое возбуждает акустомагнитные метки, находящиеся в этом поле. Метка, настроенная на ту же частоту, входит в резонанс и начинает излучать ответный сигнал. Этот ответ фиксируется приёмной антенной, после чего сигнал обрабатывается системой и при совпадении с заданными характеристиками вызывается тревожное оповещение.

Акустомагнитные метки состоят из тонкой полоски аморфного металлического сплава, помещённой в пластиковый корпус. Такая конструкция позволяет метке входить в резонанс под воздействием поля и излучать стабильный ответный сигнал в течение определённого времени (обычно около 1-2 миллисекунд) после завершения импульса возбуждения. Этот интервал (так называемое «временное окно») и используется для фиксации отклика и анализа его параметров.

Корректная работа АМ-систем требует соблюдения нескольких технических условий:

- точной калибровки антенн и согласования частот передатчика и приёмника;
- надлежащего качества электромонтажа (отсутствие перекрёстных помех и заземления);
- правильного размещения оборудования с учётом материалов стен, мебели и металлических конструкций;
- отсутствия активных источников электромагнитных помех вблизи (например, силовых трансформаторов, неэкранированных линий электропитания и т. п.).

Нарушение любого из этих условий может привести к снижению чувствительности системы, пропуску меток или, наоборот, к ложным срабатываниям. В условиях интенсивной эксплуатации, особенно при установке оборудования в многолюдных зонах или в помещениях с насыщенной электротехнической инфраструктурой, данные проблемы приобретают особую актуальность [1, с. 352].

Типы помех и источники ложных срабатываний

Акустомагнитные системы, несмотря на высокую чувствительность и устойчивость к большинству внешних воздействий, подвержены сбоям, которые проявляются в виде ложных срабатываний или пропусков меток. Эти явления снижают надёжность охранной системы, увеличивают нагрузку на технический персонал и нередко вызывают недовольство пользователей. Причины сбоев можно условно разделить на три основные группы: электромагнитные помехи, ошибки установки оборудования и внешние физические факторы.

Наиболее распространённым источником нарушений в работе АМ-систем являются электромагнитные и электрические помехи, возникающие вблизи силового оборудования, трансформаторов, кабельных трасс, приборов с импульсными источниками питания, таких как кассовые терминалы, мониторы и кондиционеры. Такие устройства создают фоновые поля, способные искажать характеристики резонансного сигнала – в частности, его частоту, фазу или амплитуду. Особенно критичным является смещение временного окна приёма, в которое система должна зафиксировать ответ от метки. В результате нарушается точность идентификации, и система может воспринимать фоновый шум как отклик.

Существенное влияние на корректность работы оказывает геометрия установки охранного оборудования. Ошибки в проектировании и монтаже антенн, такие как несоблюдение оптимального расстояния между рамками, неправильная ориентация, близость к металлическим конструкциям или отсутствие экранирования, приводят к неравномерности магнитного поля. Это может вызвать как снижение чувствительности в некоторых зонах, так и формирование «ложных» областей резонанса, что увеличивает вероятность ошибочного срабатывания [2, с. 288].

Дополнительные и часто недооцениваемые факторы связаны с внешней средой эксплуатации. Поведение людей, плотность движения, наличие металлических предметов в одежде и багаже, пронос больших сумок или тележек – всё это способно влиять на распространение сигнала. В условиях высокой проходимости или при использовании нескольких охранных систем, работающих в близких диапазонах частот, возможно возникновение взаимных наводок и сложных интерференционных

эффектов. Наконец, температурные и влажностные колебания, особенно при установке оборудования в неотапливаемых помещениях или на улице, могут приводить к дрейфу частот и изменению резонансных характеристик.

Методы интеллектуальной фильтрации сигналов

Современные акустомагнитные системы защиты, работающие на фиксированной частоте резонанса, традиционно используют простую пороговую модель обработки сигнала: при превышении заранее заданного уровня амплитуды во временном окне система инициирует срабатывание тревоги. Однако в реальных условиях эксплуатации такой подход оказывается недостаточно устойчивым к шумам, помехам и вариативности отклика. Это приводит к ложным срабатываниям или пропущенным событиям, особенно при наличии нестабильных внешних факторов. Интеллектуальные методы фильтрации сигналов предлагают альтернативу, основанную на глубоком анализе параметров сигнала и адаптивной логике реагирования.

1. Частотный и фазовый анализ сигнала

Одним из эффективных подходов к улучшению точности детекции является анализ частотного спектра входящего сигнала. В отличие от помех, имеющих широкий и нестабильный спектр, отклик акустомагнитной метки стабилен и локализован в узком диапазоне (например, 58 ± 0.2 кГц). Применение цифровых фильтров с узкой полосой пропускания позволяет исключить некорректные сигналы, не соответствующие эталонной частоте.

Дополнительную точность обеспечивает фазовый анализ. Поскольку сигнал от метки имеет устойчивую фазовую структуру, а большинство помех – хаотичны, сопоставление фазы принятого сигнала с ожидаемой позволяет отличить резонансный отклик от искажённого шума. Фазовые фильтры особенно эффективны при работе в условиях сложной электромагнитной обстановки.

2. Адаптивные алгоритмы пороговой фильтрации

Классическая логика «жёсткого порога» не учитывает изменчивость внешних условий. В отличие от неё, адаптивная фильтрация позволяет динамически корректировать параметры порога в зависимости от текущей фоновой активности, времени суток, сезона или других параметров, зарегистрированных в процессе работы системы. Это достигается путём непрерывного мониторинга статистических характеристик сигнала и автоматического обучения алгоритмов на основе накопленных данных.

Например, при повышенном уровне фонового шума система может автоматически сместить порог тревоги вверх, одновременно усилив требования к совпадению формы сигнала. В ночные часы, когда количество помех минимально, наоборот, можно использовать более чувствительные параметры, что позволяет не упустить тревожный сигнал с минимальной амплитудой [3, с. 240].

3. Временная фильтрация и сглаживание флуктуаций

Резонансный отклик метки имеет строго ограниченную временную протяжённость (обычно от 1 до 2 миллисекунд после окончания возбуждающего импульса). Применение временных окон позволяет игнорировать сигналы, зафиксированные вне ожидаемого интервала, тем самым отсеивая случайные электромагнитные наводки.

Дополнительно могут использоваться алгоритмы временного сглаживания и усреднения значений. В случае колебаний сигнала система может анализировать не отдельный импульс, а их последовательность, выявляя устойчивые закономерности. Это особенно важно при проходе метки на границе чувствительности рамки или при пересечении несколькими объектами одновременно.

4. Шаблонное распознавание и комбинированные методы

На заключительном уровне обработки возможно использование методов сопоставления формы сигнала с заранее записанным эталонным «отпечатком» резонансного отклика. Такой подход позволяет внедрять элементы шаблонного распознавания: сигнал классифицируется не только по частоте и амплитуде, но и по характеру затухания, повторяемости и симметрии. Совокупное использование всех вышеописанных методов – частотного анализа, адаптивной фильтрации, временной обработки и шаблонного сопоставления – позволяет достигать высокой устойчивости системы и минимизировать число ложных тревог даже в сложных условиях эксплуатации [4, с. 272].

Заключение

Акустомагнитные системы остаются одним из наиболее надёжных решений для периметральной охраны в условиях интенсивной эксплуатации. Однако устойчивость таких систем во многом определяется не только качеством

аппаратного обеспечения, но и эффективностью алгоритмов обработки сигнала. Классическая пороговая логика детекции часто оказывается недостаточной в реальных условиях, где воздействие внешних помех, нестабильные электромагнитные поля и ошибки монтажа могут существенно влиять на работу оборудования.

Интеллектуальные методы фильтрации сигналов, основанные на анализе частотных, фазовых и временных характеристик, а также на адаптивной корректировке параметров срабатывания, позволяют значительно повысить точность детекции, снизить количество ложных тревог и повысить общую надёжность систем охраны. Применение таких методов обеспечивает устойчивость к помехам и адаптивность к изменяющимся условиям эксплуатации, что особенно важно в многофакторной среде, характерной для современных торговых и инфраструктурных объектов.

Перспективными направлениями дальнейших исследований в данной области являются интеграция фильтрации сигналов с нейросетевыми алгоритмами классификации, автоматическое самообучение систем на основе накопленных данных, а также унификация методов обработки для совместной работы АМ-систем с другими средствами безопасности, включая видеонаблюдение и RFID-технологии.

Литература

1. Ковальчук В.И., Гуревич А.А. Технические средства охраны: учебное пособие. – М.: Академия, 2020. – 352 с.
2. Попов В.В., Губин А.Ю. Системы охранной сигнализации: теория и практика построения. – СПб.: Питер, 2018. – 288 с.
3. Кузнецов С.Н. Цифровая обработка сигналов в системах безопасности. – М.: Горячая линия – Телеком, 2019. – 240 с.
4. Ершов А.П., Левин А.М. Проектирование систем охранной сигнализации и видеонаблюдения. – М.: Радио и связь, 2021. – 272 с.

IRZHANOV Arman
Electrical and Telecommunication Systems Engineer,
"ANTI THEFT" LLP, Republic of Kazakhstan, Almaty

INNOVATIVE PERIMETER PROTECTION METHODS USING ACOUSTO-MAGNETIC SYSTEMS AND INTELLIGENT SIGNAL FILTERING

Abstract. *This article examines modern approaches to improving the accuracy and reliability of acousto-magnetic (AM) security systems through the application of intelligent signal filtering methods. It analyzes sources of interference that cause false alarms, as well as the structural and operational features of AM systems. Described techniques include spectral, phase, and temporal analysis, as well as adaptive filtering aimed at increasing system resilience to external disturbances. The proposed solutions help reduce false alarms, enhance detection selectivity, and ensure system adaptability to complex operating conditions.*

Keywords: *acousto-magnetic system, perimeter security, false alarms, signal filtering, electromagnetic interference, intelligent algorithms, adaptive processing.*

ЛЕБЕДЕВ Филипп
эксперт по кибербезопасности,
Россия, г. Москва

КИБЕРБЕЗОПАСНОСТЬ И ОБРАЗОВАНИЕ: КАК ПОДГОТОВИТЬ НОВОЕ ПОКОЛЕНИЕ СПЕЦИАЛИСТОВ

Аннотация. *В данной статье рассматривается текущее состояние образования в области кибербезопасности в Европе и необходимость подготовки нового поколения специалистов для эффективного противодействия киберугрозам. Основные цели исследования заключаются в анализе факторов, влияющих на образование в этой сфере, и в выявлении пробелов в знаниях среди студентов и преподавателей. Выявленные в исследовании недостаточная осведомленность общества о кибербезопасности и отсутствие сертификации на уровне ЕС можно обозначить как серьезные проблемы. Также исследование подчеркивает важность интеграции концепции продвинутого образования, основанной на современных технологиях, для повышения вовлеченности обучающихся и адаптации учебных программ к требованиям цифрового мира. Практическое применение результатов исследования заключается в разработке инновационных образовательных решений и повышении квалификации преподавателей, что поможет создать квалифицированные кадры, готовые к вызовам кибербезопасности.*

Ключевые слова: *кибербезопасность, образование, анализ, цифровизация, обучение, инновации.*

Сегодня образование в области кибербезопасности на всех уровнях продолжает нуждаться в поддержке и применении инновационных методов и гибких подходов к обучению. Кибербезопасность – это быстро развивающаяся сфера, за которой необходимо следить. Знания в этой области играют важную роль в цифровом обществе и требуют внимания для формирования навыков кибербезопасности у всех граждан.

Эксперты, занимающиеся вопросами экономического развития, подчеркивают необходимость овладения навыками кибербезопасности, поскольку успех в цифровой экономике будет определяться именно этими навыками. Современные инструменты, видео и электронные платформы, разработанные для обучения кибербезопасности на уровне средней школы, позволяют передавать необходимые знания с самого начала образовательного процесса, так как молодежь ежедневно сталкивается с интернет-угрозами в личной и профессиональной жизни.

Например, в 2021 году команда Центра компетенции Concordia провела исследование состояния образования в области кибербезопасности среди молодежи в ЕС – масштабный опрос в средних школах, чтобы определить значимые области кибербезопасности, которые можно включить в учебные программы [1]. Опрос охватил более 366 участников из девяти стран Евросоюза, включая учителей, учеников и родителей. Исследовательские вопросы включали:

- В какой степени темы кибербезопасности включены в школьные программы?
- Какие темы отсутствуют для повышения навыков кибербезопасности?
- Насколько старшеклассники осведомлены о кибербезопасности?
- Какие методы обучения предпочитают старшеклассники?
- Как проверить эффективность учебной программы?

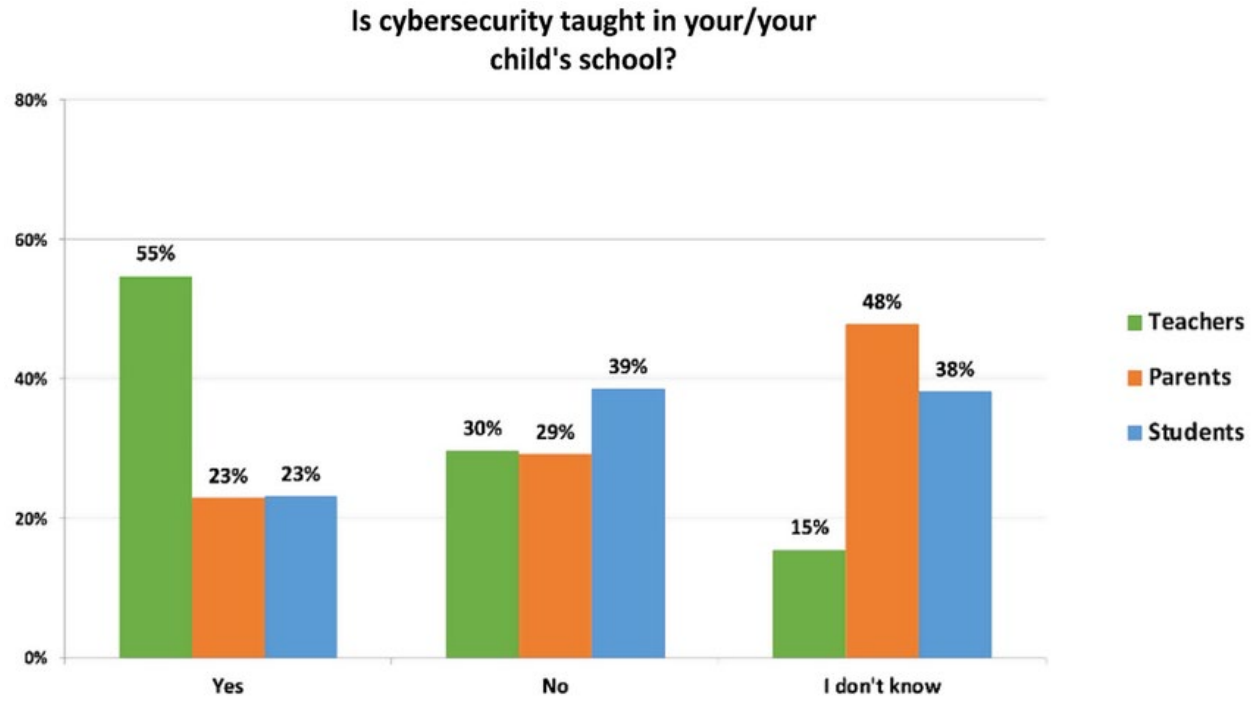

Рис. 1

Результаты показали, что многие учащиеся не уверены в своих знаниях кибербезопасности и нуждаются в дополнительном обучении. Учителя также отметили недостаток знаний в этой области, что указывает на необходимость повышения их квалификации [1].

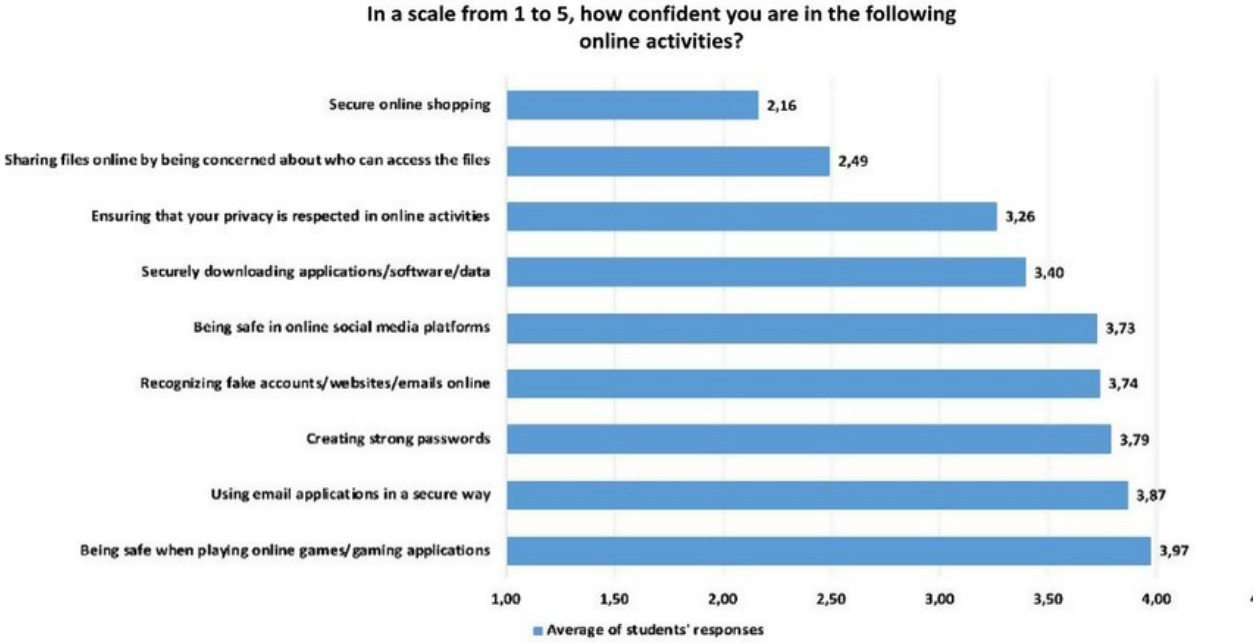

Рис. 2

К тому же интеграция кибербезопасности в среднее образование предоставит множество преимуществ, включая возможность большему числу молодых людей начать карьеру в этой области, что поможет сократить нехватку киберкадров и квалифицированной рабочей силы. Однако внедрение программ по кибербезопасности в средние школы потребует значительных временных и ресурсных затрат со стороны всех заинтересованных сторон [1].

Кибербезопасность уже не просто техническая дисциплина, а стратегическая концепция, неотъемлемая часть национальных стратегий безопасности. Отдельные европейские страны уже разработали стратегии кибербезопасности, направленные на повышение устойчивости к киберугрозам и обеспечение граждан и

компании надежными цифровыми сервисами и инструментами. В этом участвует широкий круг участников из государственного и негосударственного секторов. Однако для эффективного управления рисками в этой сфере необходимо увеличивать число квалифицированных специалистов. Крайне важно придерживаться развития образования в этой области для устранения существующих рисков. Главную роль в подготовке специалистов играют как школы, так и университеты. Образовательные учреждения должны адаптировать свои программы, чтобы готовить студентов к реальным вызовам кибербезопасности и обеспечивать им необходимые знания и навыки. Создание штата специалистов по кибербезопасности, включающего экспертов в различных областях, является важным шагом к достижению кибер-самодостаточности любой страны.

К примеру, обзор курсов по кибербезопасности в финских университетах показал, что основные темы включают технические и технологические аспекты, управление кибербезопасностью, а также социальные и человеческие факторы. Большинство курсов (более 60%) сосредоточено на технических навыках, что помогает студентам получить глубокие знания в этой области. Темы управления кибербезопасностью также важны, но вопросы, связанные с социальной и человеческой перспективами, рассматриваются реже. Анализ по Европейской таксономии кибербезопасности показал, что курсы охватывают 14 из 15 областей знаний, кроме стеганографии и водяных знаков. Часто в одном курсе объединяются несколько тем. Однако в 29 курсах внимание уделяется только одной области [2, с. 371-378].

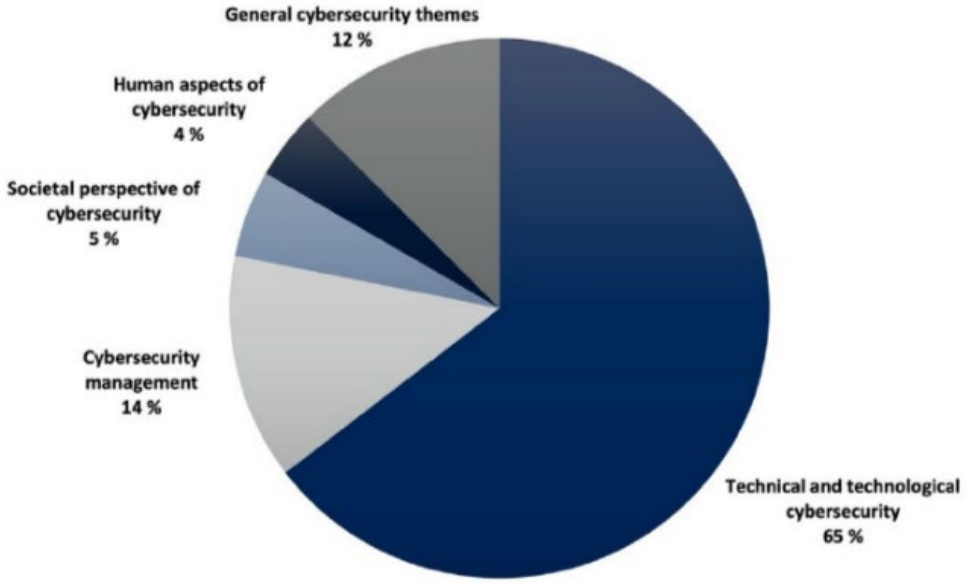

Рис. 3

Поэтому, для подготовки нового поколения специалистов в области кибербезопасности важно найти баланс между техническими навыками и более широкими аспектами, включая управление и социальные факторы.

Спрос на специалистов по кибербезопасности растет из-за увеличения цифровизации общества и расширения числа потенциальных целей для кибератак. Однако, несмотря на эту необходимость, наблюдается значительный дефицит кадров и несоответствие между навыками, приобретаемыми в процессе обучения, и теми, которые требуются в профессиональной среде.

Используя PESTLE-анализ (политический, экономический, социальный, технологический, правовой и экологический) факторов, влияющих на образование в сфере кибербезопасности в Европе, исследователям удалось классифицировать факторы, влияющие на образование и навыки в области кибербезопасности, что позволяет специалистам оценить их значимость на национальном и европейском уровнях. Результаты этого исследования показали, что недостаточная осведомленность общества о кибербезопасности и отсутствие сертификации на уровне ЕС являются серьезными проблемами в образовании. Также выявлены значительные различия между странами в

факторах, влияющих на образование в этой сфере, что подчеркивает необходимость поиска локальных решений [3, с. 1-12].

Для подготовки нового поколения специалистов в области кибербезопасности необходимо внедрение концепции продвинутого образования, основанной на современных технологиях, таких как искусственный интеллект, машинное обучение, большие данные и Интернет вещей. Эти технологии способствуют повышению персонализации и вовлеченности в процесс обучения, что является основным для формирования квалифицированных кадров. Важно учитывать, что с увеличением объема данных и взаимосвязанностью устройств возникают новые вызовы в сфере кибербезопасности, включая риски утечки информации и уязвимость к кибератакам. Поэтому образовательные программы должны не только обучать техническим навыкам, но и развивать критическое мышление и способность к быстрому реагированию на угрозы.

В рамках этого образования следует акцентировать внимание на разработке инновационных решений в области кибербезопасности, что поможет обучающимся не только осваивать теорию, но и применять знания на практике. Это может включать создание симуляций кибератак, участие в конкурсах по кибербезопасности и использование геймификации для повышения вовлеченности. И также необходимо активно повышать осведомленность о кибербезопасности среди школьников и студентов, включая темы защиты данных и киберугроз в учебные планы. Важным аспектом является сотрудничество с индустрией для обеспечения актуальности учебных программ и подготовки специалистов, готовых к вызовам современного цифрового мира [4].

Таким образом, успешная подготовка нового поколения специалистов в области кибербезопасности требует комплексного подхода, который включает современные технологии, практическое обучение и сотрудничество с индустрией. Это обеспечит соответствие образовательных программ реальным вызовам и потребностям рынка.

Литература

1. Blažič A.J., Jerman B. Teaching and learning cybersecurity for European youth by applying interactive technology and smart education. Education and Information Technologies, 2024.
2. Perälä P., Lehto M. Educating Cybersecurity Experts: Analysis of Cybersecurity Education in Finnish Universities. European Conference on Cyber Warfare and Security 23(1): P. 371-378, 2024.
3. Ricci S., Parker S., Jerabek J., Danidou Y. Understanding Cybersecurity Education Gaps in Europe. IEEE Transactions on Education PP(99): P. 1-12, 2024.
4. Dhingra M., Goyal R., Goyal S.J. Cybersecurity Challenges and Opportunities in Education 4.0. Intelligent Systems Modeling and Simulation III, 2024.

LEBEDEV Philip
cybersecurity expert, Russia, Moscow

CYBERSECURITY AND EDUCATION: HOW TO TRAIN A NEW GENERATION OF SPECIALISTS

Abstract. *This article examines the current state of cyber security education in Europe and the need to train a new generation of specialists to effectively counter cyber threats. The main objectives of the study are to analyze the factors influencing education in this area and to identify knowledge gaps among students and teachers. The lack of public awareness of cybersecurity and the lack of certification at the EU level identified in the study can be described as serious problems. The research also highlights the importance of integrating the concept of advanced education based on modern technologies to increase student engagement and adapt curricula to the demands of the digital world. The practical application of the research results lies in the development of innovative educational solutions and advanced training of teachers, which will help create qualified personnel ready for the challenges of cybersecurity.*

Keywords: *cybersecurity, education, analysis, digitalization, training, innovation.*

ХАСАНШИН Ленар Хазинурович
студент, Казанский (Приволжский) федеральный университет –
Набережночелнинский филиал, Россия, г. Набережные Челны

ИЗМЕНЕНИЕ ПОКАЗАТЕЛЕЙ РАБОТЫ ТЕПЛОВОЙ СЕТИ ПРИ ПЕРЕХОДЕ С ЦТП НА ИТП

Аннотация. *Переход от централизованных тепловых пунктов (ЦТП) к индивидуальным тепловому пунктам (ИТП) является важным этапом модернизации городских теплосетей. Этот процесс позволяет повысить энергоэффективность, снизить потери тепла и воды, а также обеспечить более стабильное и качественное отопление зданий. В данной статье рассматриваются изменения основных показателей работы тепловой сети при таком переходе, включая гидравлический режим, температурный график, потребление теплоносителя и экономические аспекты.*

Ключевые слова: *теплотехника, теплоэнергетика, тепловая сеть.*

Введение

Централизованные системы отопления традиционно используются в большинстве российских городов. Однако с развитием технологий и повышением требований к энергосбережению возникает необходимость перехода на индивидуальные тепловые пункты. Это связано с рядом преимуществ, таких как возможность точной регулировки температуры в каждом здании, снижение потерь энергии и улучшение качества обслуживания потребителей.

Методика

С помощью ПО ZuluThermo смоделирована модель тепловой сети (рис. 1), обеспечивающей теплоснабжение одного из кварталов города Нижнекамск. Теплоснабжение квартала осуществляется от ЦТП № 51, которая обеспечивает теплом два многоквартирных дома и детский садик, подключенные через элеваторный узел.

Путем поэтапного перевода потребителей ЦТП на ИТП в ZuluThermo проведены гидравлические расчеты при различной оснащенности ИТП.

Рис. 1. Расчетная модель тепловой сети г. Нижнекамск в ZuluThermo

Основные показатели работы тепловой сети

Гидравлический режим

При переходе с ЦТП на ИТП изменяется гидравлический режим тепловой сети (рис. 2). Индивидуальные тепловые пункты позволяют регулировать давление и расход теплоносителя непосредственно в точке подключения здания. Это снижает нагрузку на магистральные трубопроводы и уменьшает вероятность

возникновения аварийных ситуаций. Кроме того, улучшается распределение тепла между зданиями, что особенно важно в условиях неравномерного потребления тепла.

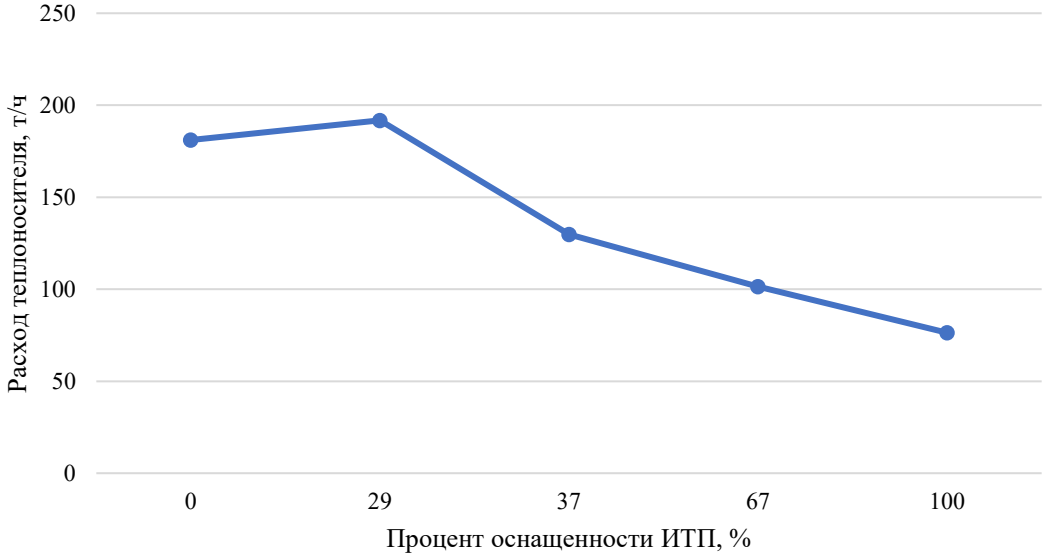

Рис. 2. Суммарный расход теплоносителя в подающем трубопроводе в зависимости от процента оснащенности ИТП

Температурный режим потребителей

При использовании ИТП появляется возможность автоматического регулирования температуры подаваемого теплоносителя в зависимости от внешних условий (температура наружного воздуха). Это обеспечивает экономию топлива и повышает комфорт жителей. Автоматическое регулирование позволяет поддерживать оптимальную температуру внутри помещений даже при резких изменениях погодных условий.

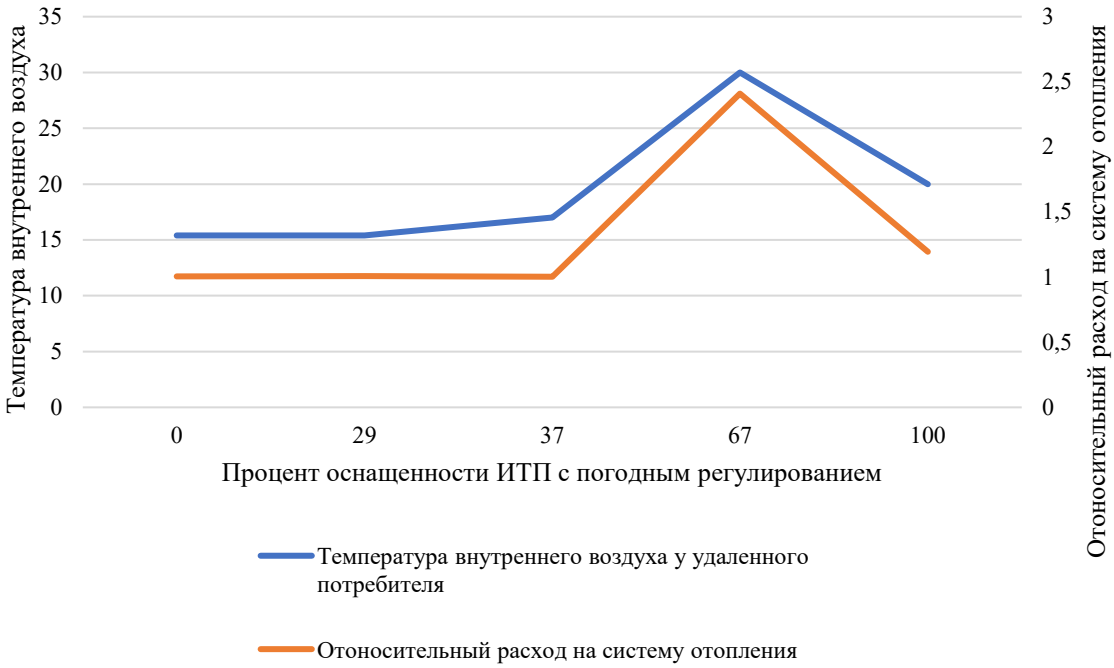

Рис. 3. Изменение температуры на самом удаленном потребителе в зависимости от процента оснащенности ИТП

На рисунке 3 представлен график изменения температуры внутреннего воздуха на самом удаленном потребителе, из графика видно, что при оснащенности ИТП в диапазоне

от 0% до 37% температура внутреннего воздуха на потребителе, присоединённом по элеваторной схеме, ниже проектной, при оснащенности ИТП в диапазоне от 37% до 67% внутренняя температура начинает расти и появляется «перетоп», в диапазоне от 67% до 100% температура внутреннего воздуха стремится к проектной.

Потребление теплоносителя

Использование индивидуальных тепловых пунктов способствует снижению общего объема потребляемого теплоносителя. Благодаря автоматической регулировке подачи тепла уменьшается количество избыточного теплоносителя, циркулирующего в системе. Это ведет к экономии ресурсов и уменьшению затрат на обслуживание сетей.

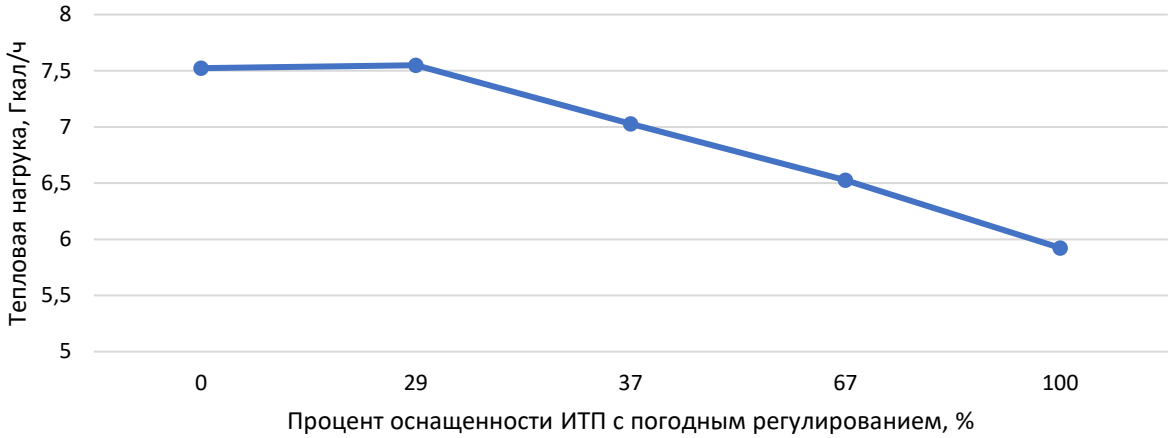

Рис. 4. Количество тепла, вырабатываемое на источнике за час в зависимости от процента оснащенности ИТП

На рисунке 4 представлен график изменения требуемой нагрузки системой теплоснабжения, в диапазоне от 0% до 29% нагрузка практически не изменилась, в диапазоне от 29% до 100% нагрузка меняется на всех этапах. Общее количество тепловой нагрузки снизилось с 7,5 Гкал/ч до 5,9 Гкал/ч или на 21,3%.

Экономические аспекты

Экономическая эффективность перехода на ИТП обусловлена несколькими факторами:

- Снижение эксплуатационных расходов: уменьшение теплопотерь и экономия энергоресурсов приводят к сокращению затрат на эксплуатацию систем отопления.
- Уменьшение количества аварий: благодаря улучшению гидравлических характеристик снижается риск возникновения аварийных ситуаций, что также влияет на общую стоимость эксплуатации.
- Повышение комфорта населения: автоматизация процессов управления отоплением улучшает качество жизни пользователей.

Однако переход требует значительных первоначальных инвестиций, связанных с заменой оборудования и модернизацией существующих систем. Важно учитывать долгосрочную перспективу и оценивать экономический эффект на протяжении всего срока службы модернизированных объектов.

Заключение

Анализ изменений показателей работы тепловой сети при переходе с ЦТП на ИТП показывает значительные преимущества нового подхода. Улучшается гидравлический режим, повышается точность поддержания температурного графика, снижается потребление теплоносителя и уменьшаются общие затраты на эксплуатацию. Несмотря на высокие начальные инвестиции, такие преобразования экономически оправданы и способствуют повышению уровня комфорта и безопасности потребителей.

Литература

1. Схема теплоснабжения муниципального образования – г. Нижнекамск на период до 2040 года.

2. Звонарева Ю.Н. Изменение параметров работы систем теплоснабжения при поэтапном внедрении АИТП / Ю.Н. Звонарева, К.С. Кузборская // Вестник Казанского государственного

энергетического университета. – 2021. – Т. 13, № 2(50). – С. 109-118. – EDN ESPPFM.

3. Филимонов А.Г. Особенности перехода Казани на АИТП при реализации комплексной программы повышения эффективности системы теплоснабжения // Вестник КГЭУ. 2019. № 2 (42). С. 127-137.

4. Запольская И.Н., Звонарева Ю.Н. Повышение эффективности систем ГВС установкой автоматизированных ИТПи // Вестник КГЭУ. 2017, № 4(36). С. 23-34.

KHASANSHIN Lenar Khazinurovich
Student, Kazan (Volga Region) Federal University – Naberezhnye Chelny branch,
Russia, Naberezhnye Chelny

CHANGES IN THE PERFORMANCE OF THE HEATING NETWORK DURING THE TRANSITION FROM TSTP TO ITP

Abstract. *The transition from centralized heating points (CSTP) to individual heating points (ITP) is an important stage in the modernization of urban heating networks. This process makes it possible to increase energy efficiency, reduce heat and water losses, and provide more stable and high-quality heating for buildings. This article discusses changes in the main performance indicators of the heating network during such a transition, including the hydraulic mode, temperature schedule, coolant consumption and economic aspects.*

Keywords: *heat engineering, heat power engineering, heating network.*

ВОЕННОЕ ДЕЛО

АЖИКЕШЕВ Артем Алексеевич
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ГЕНЕРАЛОВ Дмитрий Сергеевич
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ПОПОВ Юрий Леонидович
кандидат исторических наук, доцент, профессор,
Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

МЕТОДЫ И ФОРМЫ ДЕЯТЕЛЬНОСТИ ИНОСТРАННЫХ СПЕЦСЛУЖБ ПО ПОЛУЧЕНИЮ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Аннотация. *Данная работа представляет собой комплексное исследование, направленное на понимание методов и форм деятельности иностранных спецслужб по получению государственной тайны. Она будет полезна как для специалистов в области безопасности, так и для широкой аудитории, интересующейся вопросами защиты информации и национальной безопасности.*

Ключевые слова: *государственная тайна, шпионаж, иностранные государства, защита.*

Спецслужбы различных стран используют разнообразные методы и формы работы, направленные на сбор секретной информации, что создает значительные угрозы для национальной безопасности. В условиях глобализации и стремительного развития технологий, особенно в области информационных и кибернетических технологий, методы шпионажа и разведывательной деятельности претерпевают значительные изменения. Это делает изучение их деятельности особенно важным для понимания современных вызовов, с которыми сталкиваются государства.

Актуальность данной работы обусловлена необходимостью осознания масштабов и методов, применяемых иностранными спецслужбами, а также важностью разработки эффективных мер по защите государственной тайны. В условиях нарастающей конкуренции между государствами, а также увеличения числа кибератак, знание о том, как действуют иностранные разведки, становится критически важным для обеспечения безопасности. В данной работе будут рассмотрены общие принципы функционирования иностранных спецслужб, что позволит создать базу для дальнейшего анализа их методов и форм деятельности.

Специальные службы иностранных государств применяют разнообразные методы и формы деятельности для получения государственной тайны. Основной акцент делается на защиту информации с использованием разнообразных аспектов, включая физическую безопасность, криптографию и технологии шифрования. Защита информации предполагает соблюдение нормативных стандартов, что на практике подразумевает широкое применение как традиционных, так и современных технологий [1].

Человеческая разведка (HUMINT) и перехват электронных коммуникаций (COMINT) продолжают оставаться центральными аспектами выполнения задач спецслужб. Применение этих методов состоит в использовании агентов для сбора информации и перехвата данных, что требует от специалистов высокой степени

подготовки и конспирации [3]. Контрразведка, в свою очередь, направлена на выявление и нейтрализацию вражеских действий и обеспечивает защиту от шпионов, что является ключевым элементом в функционировании разведок [1].

Анализ открытых источников информации (OSINT) также поддерживает работу спецслужб, предоставляя возможность добывать ценную информацию без необходимости проведения тайных операций. В условиях информационной эпохи зачастую актуальные данные можно получить из публичных источников, что подчеркивает важность эффективного анализа доступных материалов [2].

Структура иностранных спецслужб включает в себя разнообразные подразделения, каждое из которых отвечает за свои специфические задачи, что позволяет более гибко реагировать на изменения в угрозах и адаптировать методы работы [3]. Таким образом, деятельность иностранных спецслужб строится на сочетании различных стратегий и технологий, направленных на защиту государственного секрета и повышения общей безопасности.

Традиционные методы шпионажа, актуальные на протяжении веков, включают в себя физические действия, секретные коммуникации и различные способы маскировки. Эти стратегии предназначены для сбора конфиденциальной информации, потенциально способной оказывать влияние на политические и экономические ситуации. Одним из любопытных методов передачи сообщений было вязание, использовавшееся как эффективное средство для сохранения секретности [1].

Сокрытие информации в коммуникациях имеет глубокие исторические корни. В античности, когда общественные структуры только формировались, передача сообщений в условиях секретности стала первоочередной задачей. Используя различные формы шифрования – от простых замен букв до создания специальных алфавитов, первоначально предназначенных для узкого круга лиц, – шпионы могли передавать сообщения, оставаясь незамеченными [3].

Сравнительно новый подход к шпионажу заключается в использовании открытых источников информации и социальных сетей. Традиционные методы шпионажа, хотя и оставались актуальными, комбинировались с другими технологиями, на основании чего возникали новые тактики. Это позволяет получать информацию как из внутренних, так и из внешних источников, создавая значительное преимущество для государственных структур и корпораций во время экономической или политической конкуренции [1].

Подводя итог, можно говорить о том, что несмотря на технологические изменения, традиционные методы, такие как шифрование и использование конфиденциальных каналов, продолжают оставаться жизнеспособными. Эти старинные практики шпионажа применяются в сочетании с новыми инструментами, позволяя адаптироваться к меняющейся обстановке и эффективно достигать целей [3].

Современные технологии шпионажа становятся особенно актуальными в условиях усиливающегося противостояния между государствами. Методы сбора информации трансформируются, включая всё более сложные технические средства и подходы. Одним из наиболее распространённых методов является распознавание голосовых данных, которое позволяет идентифицировать и отслеживать ораторов через специально разработанные алгоритмы. Это дает возможность не только фиксировать информацию, но и анализировать стиль речи, что может быть полезно для определения эмоционального состояния говорящего и выявления возможных намерений [3].

Другой важной технологией являются специальные средства радиооборудования, применяемые для удалённого доступа к компьютерам и контроля информации на них. Как сообщает The New York Times, такие методы активно используются различными спецслужбами для внедрения вредоносных программ и слежки за пользователями, что становится угрозой для частной безопасности [3]. Эти технологии позволяют злоумышленникам не только перехватывать сообщения, но и загружать данные на удалённые серверы.

Среди новейших технологий можно отметить и методы промышленного шпионажа. Как показывает практика, вербовка сотрудников конкурирующих компаний остается одним из эффективных способов получения конфиденциальной информации. Это создает необходимость для компаний усилить внутренние меры безопасности и обеспечить защиту интеллектуальной собственности [2].

Глобальные технологические тренды в шпионаже также отражают обострение конкурентной борьбы на международной арене. Поскольку шифрование становится всё более

распространённым, спецслужбы вынуждены искать адаптивные решения, которые позволят обходить новейшие технологии безопасности [2]. Таким образом, современный шпионаж интегрирует высокие технологии в процессы сбора, анализа и обработки информации, что требует от государств постоянного совершенствования своих методов защиты.

Конспиративные методы иностранных спецслужб включают целый ряд подходов, которые направлены на сохранение тайности операций и недопущение раскрытия информации о деятельности агентов. На протяжении истории такие методы использовались для заброски агентов в закрытые государства, включая СССР, где репатриация стала одною из стратегий, приведшей к регулярному выявлению иностранных шпионов. По данным, ежегодно через этот канал выявлялось от 30 до 50 агентов, что подчеркивает эффективность такого метода, но также указывает на его уязвимости в условиях высоких стандартов безопасности [3].

Помимо традиционных методов, современные спецслужбы применяют и обновленные подходы к конспирации. Конспирация в разведке включает в себя использование различных мер, направленных на защиту действий агента от наблюдения и выявления. Это требует от участников иметь специальные знания и настойчивость, опираясь на которые, они могут осуществлять деятельность, не вызывая подозрения [2]. Правила конспирации также включают разнообразие методов обеспечения безопасности, таких как использование поддельных документов и средств связи, которые могут поддерживать иллюзию нормальной жизни шпионов в обществе.

Поддержание конспиративных практик требует также от агентов умения использовать технологии для сокрытия своей деятельности. Например, многие разведывательные структуры уже используют VPN и другие методы шифрования связи для защиты данных и скрытия их местоположения, что добавляет новый уровень защиты для операций на международной арене [2].

Вместе с тем, следует отметить, что многие традиционные методы не соответствуют современным стандартам эффективности. В этом контексте необходимо развитие и совершенствование подходов, основанных на современных технологиях и методах работы, таким образом, чтобы обеспечить максимальную безопасность действий агентов и успешное выполнение задач, поставленных спецслужбами.

Кибератаки являются современным вызовом для национальной и корпоративной безопасности. С каждым годом злоумышленники становятся всё более изобретательными, использующими сложные методы для нарушения функционирования информационных систем. Такие действия могут включать повреждение или ограничение доступа к данным, а также их кражу [2]. Данный процесс требует от организаций разработки комплексных мер безопасности, способных минимизировать риск.

Основные средства защиты от кибератак включают несколько ключевых компонентов. Во-первых, антивирусные программы остаются важной защитой, но важно их регулярно обновлять для обработки новых угроз [1]. Во-вторых, криптография, как метод шифрования данных, обеспечивает защиту конфиденциальной информации, что предотвращает её перехват злоумышленниками. Брандмауэры, особенно уровня приложений, становятся критически важными для фильтрации сетевого трафика и предотвращения несанкционированного доступа [3].

Соблюдение правил кибербезопасности пользователями является обязательным. Так, осведомлённость сотрудников о потенциальных угрозах, а также обучение их правильному поведению в сети могут значительно повысить уровень защиты [1]. Важно также помнить, что кибератаки могут происходить в любое время, и при повышенной активности хакеров внедрение этих методов защиты становится неотложной задачей для организаций. С учётом всех вышеперечисленных факторов нельзя недооценивать значение кибербезопасности в текущей реальности [3].

Методы предотвращения утечек данных, представляющие собой важный аспект информационной безопасности, являются неотъемлемой частью стратегии защиты государственных и корпоративных тайн. Для эффективной реализации данной стратегии необходимо учитывать несколько ключевых направлений.

Процессуальные меры представляют собой важный аспект в управлении информационной безопасностью. Разработка строгих правил безопасности, оформление соглашений о неразглашении (NDA) с сотрудниками и мотивация работников к соблюдению норм защиты информации становятся необходимыми шагами для снижения рисков утечек [2]. Обучение

сотрудников методам предотвращения утечек также является важной частью общей стратегии, позволяя сделать их активными участниками процесса защиты информации.

Подбор сотрудников – еще один элемент, влияющий на уровень безопасности информации. Особое внимание необходимо уделять найму новых работников и их компетенциям в области информационной безопасности. Четкое определение ролей и обязанностей позволяет минимизировать вероятность инцидентов, обусловленных человеческим фактором [1]. Исследования показывают, что многие утечки данных происходят по причине недостаточной подготовки или недосмотра сотрудников, что подтверждает необходимость тщательного отбора [3].

Комплексный подход к защите информации включает сочетание технических, процессуальных и кадровых мер. Эффективное применение данных методов и технологий совместно с постоянной адаптацией политик безопасности позволяет создать надежную систему защиты, способную минимизировать риски утечек и убытков, возникающих вследствие утечки конфиденциальной информации [2]. Это становится особенно актуальным в условиях нарастающей конкуренции и динамично меняющейся угрозы со стороны иностранных спецслужб и киберпреступности.

В заключение данной работы следует подчеркнуть, что деятельность иностранных спецслужб по получению государственной тайны представляет собой сложный и многоуровневый процесс, который требует глубокого анализа и понимания. В ходе исследования были рассмотрены общие принципы функционирования этих организаций, что позволяет лучше осознать их цели и задачи. Спецслужбы, действуя в интересах своих государств, используют разнообразные методы и формы, которые можно условно разделить на традиционные и современные.

Традиционные методы шпионажа, такие как вербовка агентов, использование тайных наблюдений и внедрение в структуры, остаются актуальными и по сей день. Однако с развитием технологий и изменением геополитической обстановки, эти методы претерпевают изменения и адаптируются к новым условиям. Важным аспектом является то, что современные технологии шпионажа, включая кибершпионаж, становятся все более распространенными. Использование интернет-ресурсов, социальных сетей и других цифровых платформ позволяет спецслужбам получать доступ к информации, которая ранее была недоступна.

Конспиративные методы, применяемые иностранными спецслужбами, также заслуживают особого внимания. Эти методы направлены на скрытие истинных намерений и действий, что делает их особенно опасными. Спецслужбы используют различные приемы, чтобы избежать обнаружения, что требует от них высокой степени подготовки и профессионализма. Важно отметить, что такие действия могут иметь серьезные последствия для национальной безопасности стран, которые становятся объектами шпионской деятельности.

Кибератаки представляют собой новый вызов для безопасности государств. Они могут быть направлены как на государственные структуры, так и на частные компании, что делает их универсальным инструментом для получения информации. В условиях глобализации и цифровизации экономики, кибератаки становятся все более изощренными и трудными для предотвращения. Это подчеркивает необходимость разработки эффективных методов защиты и противодействия таким угрозам.

Методы предотвращения утечек данных и совершенствование систем безопасности являются ключевыми аспектами в борьбе со шпионской деятельностью. Важно не только реагировать на уже произошедшие инциденты, но и предугадывать возможные угрозы, создавая многоуровневую систему защиты. Это включает в себя как технические меры, так и обучение персонала, что позволяет минимизировать риски утечек информации.

Таким образом, работа подчеркивает, что деятельность иностранных спецслужб по получению государственной тайны является актуальной и многогранной проблемой, требующей комплексного подхода. В условиях постоянного изменения угроз и вызовов, важно не только изучать методы и формы шпионской деятельности, но и активно развивать системы безопасности, чтобы обеспечить защиту государственной тайны. Это требует совместных усилий как государственных структур, так и частного сектора, что в конечном итоге будет способствовать укреплению национальной безопасности и защите интересов государства.

Литература

1. 14 глаз против VPN: что нужно знать про то, как главные разведки... [Электронный ресурс] // habr.com – Режим доступа: https://habr.com/ru/companies/xeovo/articles/752010/.
2. 7 самых современных шпионских технологий – Русская семерка [Электронный ресурс] // russian7.ru – Режим доступа: https://russian7.ru/post/7-samyx-sovremennyx-shpionskix-texnologij/.
3. Совершенствование системы управления корпоративной... [Электронный ресурс] // vestnik.volbi.ru – Режим доступа: https://vestnik.volbi.ru/upload/numbers/469/article-469-4180.pdf.

AZHIKESHEV Artyom Alekseevich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

GENERALOV Dmitry Sergeevich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

POPOV Yuri Leonidovich
Candidate of Historical Sciences, Associate Professor, Professor,
Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

METHODS AND FORMS OF ACTIVITY OF FOREIGN SPECIAL SERVICES FOR OBTAINING STATE SECRETS

Abstract. *This work is a comprehensive study aimed at understanding the methods and forms of activity of foreign intelligence agencies to obtain state secrets. It will be useful both for security professionals and for a wide audience interested in information security and national security issues.*

Keywords: *state secret, espionage, foreign states, protection.*

КАШИРИН Илья Алексеевич
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ДАНИЛЕВСКИЙ Даниил Максимович
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ПОПОВ Юрий Леонидович
кандидат исторических наук, доцент, профессор,
Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ПРИМЕНЕНИЕ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. *В работе рассматривается значение биометрических технологий для защиты информации, а также их влияние на безопасность и конфиденциальность данных. Будет уделено внимание истории развитие биометрии и современным способам ее применения.*

Ключевые слова: *биометрия, защита данных, конфиденциальность, утечка данных.*

В современном мире, где информация стала одним из самых ценных ресурсов, вопросы безопасности и защиты данных приобретают особую актуальность. С каждым годом увеличивается количество кибератак, утечек данных и других угроз, что подчеркивает необходимость внедрения эффективных методов защиты. В этом контексте биометрические технологии, основанные на уникальных физических и поведенческих характеристиках человека, становятся все более популярными и востребованными. Биометрия, как наука, изучающая методы идентификации и верификации личности на основе биологических признаков, открывает новые горизонты в области безопасности информации.

История применения биометрических технологий может быть прослежена с античных времён, когда люди начали использовать индивидуальные физические характеристики для идентификации. Одним из первых примеров считается применение отпечатков пальцев в XIV веке в Китае, где они использовались для идентификации личностей и защиты документов. Эти действия заложили основы для дальнейшего развития биометрии, которая охватила такие характеристики, как ДНК, радужная оболочка глаза, голос и черты лица, став важным инструментом для подтверждения личности [1].

В XX веке биометрия стала активно развиваться благодаря прогрессу в области технологий. С появлением компьютеров и математических моделей анализа, таких как метод Eigenface, распознавание лиц стало применимо в коммерции и безопасности. С начала 2000-х годов стали доступны биометрические документы с встроенными чипами, что значительно повысило уровень безопасности при идентификации личности. Однако во многих странах информация с этих чипов ещё не используется полностью, что ограничивает её потенциал [1].

К концу XX века биометрические технологии начали внедряться в самые разные сферы: от безопасности банковских операций до контроля доступа в здания. Современные системы часто включают мультифакторную аутентификацию, основанную не только на биометрических данных, но и на других методах проверки личности. Ведущие страны начали формировать нормативно-техническую базу для стандартизации применения биометрических технологий, что способствовало интеграции различных систем и повышению их совместимости [1].

В результате исторический путь развития биометрических технологий показывает, что они прошли от простых форм идентификации до сложных и высокотехнологичных систем, способных обеспечивать безопасность и защиту информации в условиях постоянно меняющихся угроз.

Разнообразные биометрические технологии становятся неотъемлемой частью повседневной жизни, что связано с их высокой эффективностью и удобством. Они находят широкое применение в таких областях, как охрана, банковское дело и доступ к конфиденциальной информации. Наиболее распространенные методы включают распознавание отпечатков пальцев, лиц, голоса и радужной оболочки глаза. В современном мире смартфоны предлагают функции разблокировки и аутентификации на основе биометрических характеристик, что упрощает использование устройств и одновременно повышает уровень безопасности [2].

В банковском сектора, например, биометрические данные активно используются для предотвращения мошенничества и упрощения процессов аутентификации клиентов. Данные о клиентах могут быть легко защищены, а идентификация осуществляется быстро и эффективно. Применение биометрии позволяет исключить необходимость помнить пароли, что делает использование услуг более удобным и безопасным [2].

Тем не менее хорошо разработанные и правильно внедренные методы биометрической аутентификации должны соответствовать стандартам, чтобы гарантировать защиту данных. Постоянное обновление и сертификация технологий также являются важными шагами для повышения уверенности пользователей в безопасности своих данных [2]. В связи с этим биометрические технологии продолжают эволюционировать, предлагая новые возможности.

Биометрические технологии идентификации становятся все более популярными благодаря своим значительным преимуществам по сравнению с традиционными методами, такими как RFID-карты и PIN-коды. Основное внимание уделяется высокой точности аутентификации, обеспечиваемой уникальными физическими и поведенческими характеристиками каждого человека. Так, новое решение на базе рисунка подкожных вен ладони, разработанное компанией «Прософт-Биометрикс», пример подобных технологий, позволяющее значительно повысить уровень безопасности идентификации [2].

Одним из центральных преимуществ биометрии является безопасность. Процесс аутентификации на базе биометрических данных существенно снижает риск несанкционированного доступа, так как такие данные сложно подделать. В отличие от простых паролей или пластиковых карт, биометрические данные являются уникальными и неизменными, что делает их надежными инструментами для защиты информации.

Биометрия также предлагает широкий спектр возможностей для применения, включая отпечатки пальцев, распознавание радужки глаза, форму лица и звучание голоса. Каждая из этих технологий имеет свои уникальные преимущества и может быть выбрана исходя из конкретных потребностей системы безопасности [2]. Это разнообразие делает биометрические технологии универсальным инструментом, способным адаптироваться под различные нужды и задачи.

Несмотря на эти достоинства, важно понимать, что биометрические системы не являются абсолютно надежными. Существуют методы обхода данных систем, что приводит к необходимости постоянных доработок и совершенствования технологий биометрической защиты. В условиях бесконечно развивающихся методов атак невозможно полностью исключить риски, связанные с использованием биометрии [2]. Тем не менее с учетом постоянно растущих требований к безопасности и стремления к повышению удобства аутентификации, вклад биометрических технологий в защиту информации продолжает увеличиваться.

Эффективное применение биометрических технологий, таких как распознавание лиц и отпечатков пальцев, влечет за собой значительные риски, которые не должны быть игнорируемы. Одной из основных проблем является уязвимость к злоупотреблениям. Биометрические данные, будучи уникальными для каждого человека, могут быть легко украдены или подделаны с использованием различных технологий. Это создает серьезные опасения по поводу защиты личной информации и контроля над ней.

Комбинированные методы аутентификации могут повысить безопасность систем, использующих биометрические технологии. Рекомендуемая практика включает использование

паролей и двухфакторной аутентификации наряду с биометрическими данными, что может значительно уменьшить риски подделки и кражи личной информации. Число угроз со стороны киберпреступников подчеркивает необходимость внедрения дополнительных защитных мер для обеспечения безопасности клиентов и их данных.

Наконец, не стоит забывать о рисках, связанных с длительным хранением биометрических данных. Увеличение срока хранения таких данных до 100 лет создает непредсказуемость последствий в управлении и защите личной информации, особенно в условиях постоянно развивающихся технологий. Важно отметить, что ни одна биометрическая система не может гарантировать абсолютную безопасность, и необходимы комплексные подходы для минимизации потенциальных угроз.

Таким образом, разработчики и власти должны учитывать текущие риски и работать над созданием безопасных и эффективных систем защиты биометрических данных. Интеграция современных технологий и соблюдение строгих стандартов безопасности может уменьшить вероятность злоупотреблений и повысить доверие к таким системам.

Единая биометрическая система (ЕБС) представляет собой важный шаг в использовании биометрических технологий для идентификации и аутентификации граждан России. Созданная для того, чтобы упростить доступ к государственным и финансовым услугам, она играет значительную роль в повышении уровня удобства и безопасности пользователей. Разработка системы началась в 2017 году по инициативе Банка России и Минцифры, с активным участием «Ростелекома» [4].

Система функционирует путем сбора биометрических данных, включая изображения лиц и записи голосов, которые потом хранятся в зашифрованном виде. Все организации, осуществляющие сбор биометрических данных, обязаны передавать их в ЕБС, что обеспечивает централизованный подход к обработке и хранению информации [4]. Некоторые финансовые учреждения получают доступ к данным лишь в виде математических кодов, что минимизирует риски утечек личной информации и значительно повышает уровень защиты.

Однако Россия не единственное государство, которое рассматривает биометрические технологии как средство упрощения и улучшения государственных услуг. В многих других странах также внедряются подобные решения, что свидетельствует о глобальном тренде в использовании биометрии для идентификации пользователей. Таким образом, ЕБС может стать моделью для аналогичных инициатив в других странах, продвигая идеи о безопасности и удобстве [4].

В рамках ЕБС пользователи могут по-прежнему получать услуги как дистанционно, так и непосредственно, что отражает современные подходы в сфере цифровизации и обслуживания граждан [4]. Применение биометрических технологий в управлении государственными сервисами может менять общественное восприятие взаимодействия с государственными структурами, повышая уровень доверия и удовлетворенности от услуг.

Актуальность биометрических технологий, особенно в сфере защиты информации, продолжает расти. Сложные алгоритмы обработки биометрических данных и их интеграция в системы аутентификации делают возможным более безопасное взаимодействие между пользователями и различными сервисами. Ожидается, что в ближайшие несколько лет технологии биометрической идентификации, такие как распознавание лиц и анализа голоса, станут неотъемлемой частью общественной инфраструктуры и коммерческого сектора [3].

Существует множество направлений, где биометрия находит свое применение. Одним из них является контроль доступа к товарам с возрастными ограничениями, что говорит о многофункциональности биометрических решений. Однако, усиление использования таких технологий приводит к увеличению требований по защите данных. Как показывают эксперты, безопасность данных на уровне, необходимом для защиты критически важных технологий, станет обязательной.

Как правило, устойчивость и репутация компании во многом зависят от того, насколько безопасными будут биометрические системы, которые они используют. Эффективное управление данными только тогда возможно, когда соблюдаются все обязательства по защите информации, и пользователи могут доверять новым технологиям [3]. Таким образом, внедрение биометрических технологий должно быть основано на принципах

прозрачности и соблюдения прав граждан, так как это будет способствовать более широкому их принятию и использованию в будущем. Технологии, которые предлагают реальный уровень безопасности, могут стать катализатором для дальнейшего внедрения в различные сферы жизни.

Современные применения биометрии охватывают широкий спектр областей, включая финансовые услуги, государственные учреждения, системы безопасности и даже повседневные устройства, такие как смартфоны. Эти технологии обеспечивают высокий уровень защиты, позволяя идентифицировать пользователей с высокой точностью и минимизируя риски, связанные с кражей личных данных. Преимущества биометрических технологий очевидны: они обеспечивают удобство, скорость и надежность, что делает их привлекательными для пользователей и организаций.

Однако, несмотря на все положительные аспекты, внедрение биометрии также сопряжено с рядом рисков и вызовов. Одним из основных является угроза утечки биометрических данных, которые, в отличие от паролей, невозможно изменить. Это создает серьезные проблемы в случае их компрометации. Кроме того, существует риск создания систем слежения и нарушения прав человека, что поднимает важные этические вопросы. Важно учитывать, что биометрические данные могут быть использованы не только для защиты, но и для контроля, что вызывает опасения у общества.

В контексте России стоит отметить развитие Единой биометрической системы (ЕБС), которая направлена на улучшение защиты данных граждан. Однако, несмотря на ее преимущества, необходимо учитывать и возможные негативные последствия, такие как вопросы конфиденциальности и возможность принудительного использования биометрических данных. Общество должно быть готово к обсуждению этих вопросов и выработке четких норм и правил, регулирующих использование биометрических технологий.

Таким образом, биометрические технологии представляют собой мощный инструмент для защиты информации, однако их внедрение требует взвешенного подхода. Необходимо учитывать как положительные, так и отрицательные аспекты, чтобы обеспечить безопасность и конфиденциальность данных. В будущем важно продолжать исследовать и развивать биометрические технологии, одновременно уделяя внимание этическим и правовым вопросам, связанным с их использованием. Это позволит создать безопасное и комфортное пространство для всех пользователей, где биометрия будет служить не только средством защиты, но и гарантией соблюдения прав и свобод человека. В конечном итоге, успешное применение биометрических технологий зависит от баланса между инновациями и ответственностью, что является ключевым аспектом для формирования безопасного цифрового будущего.

Литература

1. Биометрическая аутентификация – что это такое и зачем она нужна [Электронный ресурс] // rt-solar.ru – Режим доступа: https://rt-solar.ru/events/blog/3616/.

2. Преимущества биометрических методов идентификации… [Электронный ресурс] // www.cta.ru – Режим доступа: https://www.cta.ru/articles/cta/obzory/tekhnologii/124324/.

3. Будущее биометрических технологий для аутентификации… [Электронный ресурс] // www.aktiv-company.ru – Режим доступа: https://www.aktiv-company.ru/press-center/publication/2024-06-22.html.

4. Единая биометрическая система [Электронный ресурс] // digital.gov.ru – Режим доступа: https://digital.gov.ru/en/activity/czifrovaya-identifikacziya/edinaya-biometricheskaya-systema.

KASHIRIN Ilya Alekseevich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

DANILEVSKY Daniil Maksimovich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

POPOV Yuri Leonidovich
Candidate of Historical Sciences, Associate Professor, Professor,
Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

THE USE OF BIOMETRIC TECHNOLOGIES TO PROTECT INFORMATION

Abstract. *The paper examines the importance of biometric technologies for information protection, as well as their impact on data security and confidentiality. Attention will be paid to the history of biometrics development and modern ways of its application.*

Keywords: *biometrics, data protection, privacy, data leakage.*

КУЛЬМАНОВ Эмиль Камилевич
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ХАЛИУЛЛИН Радмир Дамирович
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ПОПОВ Юрий Леонидович
кандидат исторических наук, доцент, профессор,
Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

БЕЗОПАСНОСТЬ ДАННЫХ В ОБЛАЧНЫХ ХРАНИЛИЩАХ: УГРОЗА УТЕЧЕК И МЕТОДЫ ЗАЩИТЫ

Аннотация. *В данной работе будет рассмотрено множество аспектов, связанных с безопасностью данных, включая типы угроз, с которыми сталкиваются облачные хранилища, и методы защиты, которые могут быть применены для минимизации рисков.*

Ключевые слова: *государственная тайна, чрезвычайная ситуация, особенность, защита, закон.*

В условиях стремительного роста популярности облачных технологий вопрос безопасности данных в облачных хранилищах становится особенно актуальным. Облачные сервисы предоставляют пользователям удобный доступ к данным и приложениям, однако с этим удобством приходят и серьезные риски. Утечки информации, кибератаки и несанкционированный доступ к данным представляют собой лишь некоторые из угроз, с которыми сталкиваются организации и частные пользователи. В связи с этим, необходимость внедрения современных методов защиты данных становится неотъемлемой частью стратегии управления информационной безопасностью.

Актуальность проблемы безопасности данных в облачных хранилищах обусловлена не только увеличением объема хранимой информации, но и разнообразием типов угроз, которые могут возникнуть в процессе использования облачных технологий.

Проблемы конфиденциальности бьют по нервам половины пользователей облачных сервисов, которые беспокоятся о безопасности своих данных. Мировой средний показатель утечек личных данных во время инцидентов составляет 2,52 миллиона записей, тогда как в России этот показатель немного ниже – 2,38 миллиона [1]. Важно отметить, что более 99% утечек в России имеют умышленный характер, что указывает на необходимость более серьезного подхода к защите информации [1].

Ситуация настоятельно требует более активных шагов со стороны бизнеса, который все еще упускает возможности по улучшению своего информационного безопасности. В условиях растущих угроз важно интегрировать радикальные изменения в корпоративные стратегии и тактики управления безопасностью, чтобы перейти от реактивного к проактивному подходу в защиту данных.

Облачные хранилища, несмотря на их удобство и эффективность, подвержены различным угрозам, которые могут привести к утечкам и несанкционированному доступу к данным пользователей. Одна из наиболее значительных угроз заключается в утечке данных, которая может произойти из-за взломов серверов, неоптимальных настроек безопасности или известных уязвимостей в программном обеспечении. Такие инциденты не только ставят под угрозу конфиденциальную информацию, но и могут существенно повредить репутации компаний, что в свою очередь может привести к

финансовым потерям и снижению доверия со стороны клиентов [4].

Неавторизованный доступ также представляет собой серьезную проблему. Злоумышленники могут использовать слабые места в системе для получения доступа к данным, в то время как прежние пользователи или внутренние сотрудники могут случайно или намеренно раскрыть конфиденциальную информацию. Это подчеркивает важность адекватного контроля доступа и постоянного мониторинга активных пользователей систем.

Вредоносное программное обеспечение, такое как вирусы и трояны, также представляет собой опасность для облачных хранилищ. Эти программы могут проникнуть в системы через зараженные файлы, что может привести к повреждению данных или потере информации [3]. Необходимо постоянно отслеживать и одновременно обновлять антивирусное программное обеспечение, чтобы минимизировать эти риски.

Создание программистами безопасных архитектур, использование шифрования данных и регулярное обучение сотрудников основам кибербезопасности являются необходимыми мерами для защиты от вышеуказанных угроз. Объединив технологии и грамотные практики, компании могут значительно улучшить уровень защищенности своих облачных ресурсов.

Шифрование данных в облачных хранилищах имеет стратегическое значение для обеспечения конфиденциальности и защиты информации от несанкционированного доступа. Наиболее распространенные подходы к шифрованию включают самостоятельное шифрование, облачное шифрование с встроенными функциями и использование сторонних приложений.

Облачные сервисы, такие как AWS, предлагают встроенные инструменты для шифрования, однако многие пользователи не знакомы с этими функциями. Это подчеркивает необходимость повышения осведомленности о доступных возможностях шифрования, чтобы максимально защитить данные [2]. Важно отметить, что в зависимости от реализации облачного шифрования пользователи могут столкнуться с ограничениями, которые повлияют на их возможности управления данными, что делает ситуацию более уязвимой.

Сторонние приложения также становятся популярными для шифрования данных перед загрузкой в различные облачные хранилища. Эти решения позволяют шифровать данные независимо от платформы, на которой они хранятся. Компании могут использовать такие инструменты, чтобы создать многоуровневую защиту данных, минимизируя риски потери конфиденциальности [1].

Последствия недостаточной безопасности данных в облаках очень серьезны. Утечки информации могут привести к репутационным потерям и финансовым убыткам для организаций. Насущной задачей остается развитие технологий шифрования, чтобы следовать актуальным требованиям законодательства и стандартам безопасности. Каждая компания должна принимать во внимание свои специфические потребности и выбирать те методы шифрования, которые лучше всего соответствуют их целям и задачам [3].

Двухфакторная аутентификация (2FA) представляет собой важный метод повышения безопасности в процессе работы с облачными хранилищами. Она требует от пользователей подтверждения своей личности с помощью двух независимых способов, что значительно усложняет задачу злоумышленников. Например, по данным Microsoft, 2FA может блокировать до 99,9% автоматизированных атак на аккаунты, что подтверждает его эффективность в контексте защиты данных [2].

Одним из распространенных способов 2FA является использование комбинации пароля и кода, который пользователь получает через SMS или специальные приложения. Это обеспечивает дополнительный уровень защиты, так как злоумышленник должен получить доступ не только к паролю, но и к устройству, на которое отправляется код. Существуют и другие варианты, включая биометрические методы и USB-ключи, что делает 2FA гибким инструментом для различных ситуаций и потребностей [2].

Эффективность 2FA заключается в том, что он сочетает два типа идентификационных данных: что-то, что знает пользователь (например, пароль), и что-то, что у него есть (например, телефон для получения кода). Это создает дополнительные преграды для потенциальных злоумышленников, которые могут попытаться получить доступ к аккаунту [2].

Таким образом, внедрение двухфакторной аутентификации в систему безопасности облачных хранилищ представляется не только актуальным, но и жизненно необходимым шагом для защиты личных данных пользователей. В условиях постоянного роста угроз кибератак и утечек данных, 2FA становится эффективным инструментом, позволяющим минимизировать риски и обеспечивать уровень безопасности, соответствующий современным требованиям [3].

Обеспечение безопасности облачных хранилищ требует комплексного подхода, который включает в себя внедрение множества мероприятий, призванных минимизировать риски утечек данных и кибератак. Одной из первых практик является безопасный доступ и управление идентификацией пользователей. Использование многофакторной аутентификации значительно повышает уровень контроля доступа, гарантируя, что к данным облака получают доступ только авторизованные пользователи [1].

Шифрование данных является важнейшим методом защиты в облаке, как при передаче (In-transit), так и при хранении (At-rest). Применение протоколов TLS/SSL для шифрования данных во время их передачи минимизирует риск перехвата, а шифрование данных в самом облаке защищает их от потенциальной утечки [3]. Эффективность этой методы подтверждена многими исследованиями и практикой.

Внедрение систем предотвращения утечек данных (DLP) помогает контролировать работу сотрудников и предотвращает несанкционированный доступ к информации. Этот метод позволяет отслеживать использование данных и фиксировать подозрительную активность [2].

Также важно иметь стратегии резервного копирования и восстановления данных. Регулярные резервные копии гарантируют возможность восстановления данных в случае инцидентов, связанных с потерей или повреждением информации. Планы восстановления должны быть четко прописаны и протестированы на практике.

Наконец, выбор надежного поставщика облачных услуг имеет значение для обеспечения безопасности данных. Партнеры должны продемонстрировать отлаженные процессы безопасности и следование актуальным стандартам защиты данных, что особенно важно в контексте соблюдения законодательства о защите информации [1]. Таким образом, системный подход к безопасности облачных хранилищ значительно снижает риски утечек данных и создает безопасную среду для работы с информацией.

Будущее безопасности данных в облачных хранилищах будет определяться интеграцией современных подходов и технологий, таких как искусственный интеллект (ИИ) и машинное обучение (МЛ). Эти технологии помогут не только в мониторинге, но и в автоматическом реагировании на киберугрозы, что крайне важно в условиях растущего числа утечек данных. Например, в 2018 году произошло более 3000 утечек данных, затронувших более 136 миллионов записей, что наглядно иллюстрирует актуальность проблемы [2].

Основное направление, на которое следует обратить внимание, – это автоматизация процессов безопасности с использованием ИИ и МЛ. Это позволит выявлять и предотвращать атаки в реальном времени, минимизируя время реакции и снижая возможность человеческой ошибки [3]. Важно отметить, что такая автоматизация не должна заменять человеческое участие, а наоборот, дополнять его, обеспечивая многослойный защитный механизм.

Адаптация к новым угрозам остается основным приоритетом для бизнеса, который должен активно развивать свои стратегии кибербезопасности. Необходимо учитывать не только внешние угрозы, но и внутренние, что в условиях удаленной работы становится особенно актуальным. Статистика показывает, что большинство утечек данных происходит из-за человеческого фактора, поэтому обучение и повышение осведомленности пользователей о киберугрозах становится обязательным.

В заключение, будущее безопасности данных в облачных хранилищах зависит от комплексного и адаптивного подхода, сочетая инновационные решения и постоянное обучение. Необходимость защищать данные становится неоспоримой, и только эффективно комбинируя технологии, практики и человеческий ресурс, можно достичь желаемого уровня безопасности в современной цифровой среде.

В заключение данной работы следует подчеркнуть, что безопасность данных в облачных хранилищах является одной из наиболее актуальных и сложных проблем современного

информационного общества. С каждым годом количество пользователей облачных сервисов растет, что, в свою очередь, увеличивает объемы хранимой информации и, соответственно, риски, связанные с ее утечкой. Угрозы, такие как кибератаки, фишинг, вредоносное ПО и внутренние угрозы, становятся все более изощренными, что требует от организаций постоянного внимания к вопросам защиты данных.

Одним из ключевых аспектов, рассмотренных в работе, является шифрование данных. Этот метод защиты информации позволяет значительно снизить риски утечек, так как даже в случае несанкционированного доступа к данным, злоумышленник не сможет их прочитать без соответствующего ключа. Шифрование должно применяться как на уровне хранения данных, так и при их передаче, что обеспечивает комплексный подход к безопасности.

Двухфакторная аутентификация (2FA) также играет важную роль в защите облачных хранилищ. Этот метод добавляет дополнительный уровень безопасности, требуя от пользователей подтверждения своей личности не только с помощью пароля, но и с помощью второго фактора, например SMS-кода или биометрических данных. Внедрение 2FA значительно снижает вероятность несанкционированного доступа к учетным записям, что особенно важно в условиях растущих угроз.

Лучшие практики на уровне инфраструктуры также не следует игнорировать. Это включает в себя регулярные обновления программного обеспечения, мониторинг активности пользователей и систем, а также оценку рисков. Использование современных инструментов для анализа и управления безопасностью может помочь в выявлении уязвимостей и своевременном реагировании на инциденты.

Наконец, будущее безопасности данных в облаках будет зависеть от развития технологий и методов защиты. С появлением новых угроз необходимо будет адаптировать существующие подходы и разрабатывать инновационные решения. Важно, чтобы компании не только следили за текущими тенденциями, но и предугадывали возможные риски, что позволит им оставаться на шаг впереди злоумышленников.

Таким образом, безопасность данных в облачных хранилищах требует комплексного подхода, включающего в себя как технические, так и организационные меры. Только при условии постоянного внимания к вопросам защиты информации можно минимизировать риски утечек и обеспечить надежное сохранение критически важной информации. В условиях стремительного роста популярности облачных технологий этот вопрос остается актуальным и требует постоянного изучения и внедрения новых методов защиты.

Литература

1. 10 лучших практик облачной безопасности в 2025 году [Электронный ресурс] // tr-page.yandex.ru – Режим доступа: https://tr-page.yandex.ru/translate?lang=enru&url=https://www.geeksforgeeks.org/cloud-security-best-practices/.

2. Главные угрозы облачной безопасности | Xelent | Xelent [Электронный ресурс] // www.xelent.ru – Режим доступа: https://www.xelent.ru/blog/glavnye-ugrozy-oblachnoy-bezopasnosti/.

3. Двухфакторная аутентификация: плюсы... – Контур.Эгида [Электронный ресурс] // kontur.ru – Режим доступа: https://kontur.ru/aegis/blog/55728-dvuhfaktornaya_autentifikaciya.

4. Насколько безопасны облачные решения – DeoniX [Электронный ресурс] // deonix.kz – Режим доступа: https://deonix.kz/news/naskolko-bezopasny-oblachnye-resheniya/.

KULMANOV Emil Kamilevich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

KHALIULLIN Radmir Damirovich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

POPOV Yuri Leonidovich
Candidate of Historical Sciences, Associate Professor, Professor,
Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

DATA SECURITY IN CLOUD STORAGE: THE THREAT OF LEAKS AND PROTECTION METHODS

Abstract. *This paper will cover many aspects related to data security, including the types of threats faced by cloud storage and the protection methods that can be applied to minimize risks.*

Keywords: *state secret, emergency, feature, protection, law.*

КОНОВАЛОВ Михаил Вадимович
курсант/военнослужащий,
Ярославское высшее военное училище противовоздушной обороны имени
Маршала Советского Союза Л. А. Говорова, Россия, г. Ярославль

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ НАВЕДЕНИЯ ВЫСОКОТОЧНОГО ОРУЖИЯ С ПАССИВНОЙ ГОЛОВКОЙ САМОНАВЕДЕНИЯ

Аннотация. *Рассматривается сущность и актуальность противодействия противорадиолокационным ракетам, способы и методы противодействия. Производиться анализ метода постановки когерентной помехи головке самонаведения противорадиолокационной ракеты.*

Ключевые слова: *противорадиолокационная ракета, головка самонаведения, когерентная помеха.*

Анализ современных локальных войн и вооруженных конфликтов показывают, что первому удару в воздушно-наступательной операции подвергаются подразделения противовоздушной обороны (ПВО) при этом широко используются противорадиолокационные ракеты (ПРР) [1, с. 3-25]. Высокая эффективность применения данного высокоточного оружия определяет важную задачу противодействия ПРР.

В данной статье рассматривается способ формирования пространственно-разнесенной помехи двумя источниками когерентных сигналов, в литературе встречается другое название – когерентная двухточечная помех.

Когерентная двухточечная помеха – это суммарная электромагнитная волна, создаваемая связанными по фазе сигналами разнесенных в пространстве источников излучения [2].

Основным измерительным элементом пассивной системы самонаведения ПРР является моноимпульсный пеленгатор, как известно данные устройства оценивают направление на источник излучения по положению нормали к принимаемому фазовому фронту электромагнитной волны. Сущность воздействия когерентной помехи заключается в искажении фазового фронта принимаемой пеленгатором ПРР суммарной электромагнитной волны сигналов двух источников излучения, что в свою очередь приводит к ошибочной оценке направления на РЛС-цель и в конечном итоге к промаху противорадиолокационной ракеты [2].

Рис. Траектория полета ПРР при постановке когерентной помехи на ГСН

Применение метода искажения фазового фронта электромагнитной волны, при котором сигналы излучаются двумя источниками, разнесенными на местности, является одним из более перспективных в настоящее время.

Значение ошибки определения углового положения РЛС-цели формируемой когерентной

двухточечной помехой определяется выражением:

$$\vartheta = \tan^{-1}\left[\frac{d*cos(\beta)}{2r_0}\frac{1-\delta^2}{(1+\delta^2+2\delta\cos(2\pi d\sin(\beta)+\Delta\varphi))}\right], \quad (1)$$

Где: d – значение базы между источниками излучения; β – азимутальное направление от центра базы на ПРР; r_0 – расстояние от центра базы до ПРР; δ – отношение амплитуд сигналов источников излучения; $\Delta\varphi$ – разность фаз сигналов источников излучения.

Равносигнальное направление в общем случае смещено относительно центра базы между целями на величину угловой ошибки. Предположим, что дальности r_1, r_2 от постановщиков помех до антенны пеленгатора отличаются от нормали примерно на одну и ту же величину. Пеленги целей, отсчитываемые относительно равносигнального направления пеленгатора равны:

$$\varepsilon_1 = -\left(\frac{\Delta\theta_1}{2} + \vartheta\right) \text{ и } \varepsilon_2 = +\frac{\Delta\theta_2}{2} - \vartheta, \quad (2)$$

Где: $\Delta\theta$ – угловой разнос равносигнального направления относительно цели; ϑ – значение ошибки определения углового положения.

Если когерентные помехи синфазны ($\Delta\varphi = 0$), то из выражения (2) следует, что:

$$\vartheta = \frac{\Delta\theta}{2}\left(\frac{1-\beta}{1+\beta}\right), \quad (3)$$

Из выражения (3) следует, что при $\beta = 1$ пеленгатор следит за центром базы (амплитудный центр, образованный двумя источниками излучения одинаковых по амплитуде колебаний). При $\beta \neq 1$ равносигнальное направление пеленгатора следит за некоторой точкой внутри базы.

Анализ показывает, что когерентные помехи при условии $\beta = 1$, $\Delta\varphi = 0$ и $r_1 \approx r_2 \approx r$ являются эффективным средством увода радиопеленгаторов любых типов, в частности моноимпульсных пеленгаторов, за базу источников излучения. Единственное, что необходимо для эффективности противодействия при помощи такой помехи это условие нахождения обоих источников излучения в главном лепестке диаграммы направленности антенны пеленгатора.

Заключение

Таким образом, результаты исследования показали, что применения способа постановки когерентной помехи на пассивную систему самонаведения ПРР с помощью двух пространственно-разнесенных источников излучения позволяет исключить поражение РЛС импульсного типа рассмотренным вооружением предполагаемого противника, однако сложность постановки когерентной помехи заключается в сложности построения аппаратуры, обеспечивающей устойчивое амплитудно-фазовое распределение и реализации точных задержек сигнала. В дальнейшем необходимо разработать предложения по реализации более точной и устойчивой аппаратуры для создания когерентной помехи.

Литература

1. Куприянов А.И. Радиоэлектронная борьба: ракеты против РЛС, 2016 г. – С. 3-25. – Текст: непосредственный.

2. Вакин С.А., Шустов Л.Н. Основы радиопротиводействия и радиотехнической разведки. 1968 г. – Текст: электронный.

KONOVALOV Mikhail Vadimovich

Cadet/Soldier, Yaroslavl Higher Military School of Air Defense named after Marshal of the Soviet Union L. A. Govorov, Russia, Yaroslavl

DEVELOPMENT OF A SIMULATION MODEL FOR THE GUIDANCE OF HIGH-PRECISION WEAPONS WITH A PASSIVE HOMING HEAD

Abstract. *The article considers the nature and relevance of counteraction to anti-radar missiles, methods and techniques of counteraction. An analysis of the method of setting a coherent interference on the homing head of an anti-radar missile is carried out. A conclusion is made about the prospects and effectiveness of this method.*

Keywords: *anti-radar missile, homing head, coherent interference.*

ЛУТЕНКО Евгений Николаевич
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

МОХИРЕВ Константин Павлович
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ПОПОВ Юрий Леонидович
кандидат исторических наук, доцент, профессор,
Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Аннотация. *В работе будет рассмотрено значение государственной тайны в международных отношениях. Мы рассмотрим международные соглашения и конвенции, которые регулируют вопросы защиты конфиденциальной информации, а также роль России в международном сотрудничестве по защите государственной тайны.*

Ключевые слова: *государственная тайна, международные отношения, соглашения, защита, закон.*

В условиях стремительной глобализации и углубления международных отношений вопросы безопасности становятся особенно актуальными. Одним из ключевых аспектов этой безопасности является защита государственной тайны, которая представляет собой совокупность сведений, доступ к которым ограничен в интересах обеспечения безопасности государства. В современных условиях, когда информация становится важнейшим ресурсом, а технологии позволяют осуществлять быстрый и несанкционированный доступ к конфиденциальным данным, необходимость в международном сотрудничестве в области защиты государственной тайны становится неоспоримой.

Актуальность данной работы обусловлена тем, что в условиях глобализации и увеличения числа транснациональных угроз, таких как терроризм, киберпреступность и шпионаж, государства сталкиваются с необходимостью совместной работы по защите своих интересов. Важность защиты государственной тайны не ограничивается лишь национальными рамками; она требует координации усилий на международном уровне. В этой связи работа будет посвящена анализу ключевых аспектов международного сотрудничества в области защиты государственной тайны, включая правовые и организационные механизмы, которые используются для обеспечения конфиденциальности информации.

Государственная тайна в международных отношениях является важным инструментом, направленным на защиту национальных интересов. В условиях глобализации и роста межгосударственного взаимодействия необходимость охраны такой информации становится особенно актуальной. Некоторые категории сведений, относящихся к государственной тайне, защищают военные, экономические и политические интересы страны, подрывающие интеллектуальную и стратегическую безопасность.

Одной из важнейших задач государства является обеспечение баланса между необходимостью открытости в международных отношениях и защитой секретной информации. В разных странах существуют свои подходы к классификации и охране государственной тайны, что может накладывать ограничения на международное сотрудничество в этой области. В России виды информации, относящиеся к государственной тайне, четко определены законом, что позволяет установить четкие границы доступа и секрета [1]. Нарушение этой защиты влечет за собой не только юридические

последствия, но и угрозы национальной безопасности.

Источники, из которых черпаются знания о государственной тайне, все более активно используются в практике международных отношений. Важно осознавать, что существует множество вызовов, огромный объем которых приходится на взаимодействие между государствами в контексте защиты секретной информации, что делает это направление значимым в современных международных отношениях.

Закон Российской Федерации «О государственной тайне» от 21 июля 1993 года определяет правовые основы защиты сведений, относящихся к государственной тайне. Он включает в себя определения, классификацию и порядок доступа к информации, которую необходимо защищать от раскрытия. Закон создает основу для функционирования системы защиты государственной тайны, в которую входят специализированные органы и процедуры, направленные на предотвращение несанкционированного доступа к секретной информации [1].

Система защиты государственной тайны включает в себя разнообразные меры, такие как технические, организационные и юридические методы. Например, использование современных технологий криптографии и специальных средств защиты информации позволяет эффективно защищать данные от кибератак и утечек. Правильное применение данных средств будет способствовать укреплению безопасности и конфиденциальности информации, имеющей значение для национальной безопасности [1].

Организационные механизмы защиты государственной тайны в России базируются на нормативных актах, таких как Федеральный закон «О государственной тайне» и других регулирующих документах. Система охраны включает в себя не только органы государственной власти, но и методы работы, направленные на предотвращение утечек секретной информации и защиту от угроз, в том числе технической разведки других стран [2].

Ключевым аспектом является оформление допуска к секретной информации. Порядок предоставления таких прав зависит от строгих проверок и условий, что создает необходимую защиту для информации, представляющей интерес для государственной безопасности [2]. Лица и организации, допущенные к государственной тайне, обязаны соблюдать законодательные нормы и отвечать требованиям, установленным для работы с секретными сведениями.

Немаловажную роль в механизме защиты играют контрольные органы, которые не только устанавливают правила для работы с государственной тайной, но и контролируют их соблюдение. Это позволяет оперативно реагировать на возможные нарушения и минимизировать риски утечки информации [2].

Регулирование и международное сотрудничество также являются важными аспектами системы защиты. Взаимодействие с международными договорами и соглашениями позволяет унифицировать подходы к защите информации, что особенно актуально в условиях глобализации и увеличения числа транснациональных угроз [2].

Таким образом, организационные механизмы защиты государственной тайны в России можно рассматривать как динамичную и комплексную систему, в которой сочетаются правовые, организационные и технические меры, направленные на адекватное реагирование на современные вызовы.

Международные соглашения о защите государственной тайны представляют собой важный инструмент, позволяющий государствам совместно обеспечивать безопасность и защиту конфиденциальной информации. Эти соглашения формируют правовые рамки для обмена сведениями, относящимися к государственной тайне, и определяют порядок их защиты, что особенно актуально в условиях глобализации и роста угроз безопасности [3].

Процедуры, касающиеся засекречивания и рассекречивания необходимой информации, играют ключевую роль в повышении эффективности международного сотрудничества. Регламентация этих процессов позволяет минимизировать риски утечки данных и упрощает взаимодействие между государственными органами разных стран [3]. В контексте России эти процедуры регулируются законодательством, обеспечивающим правовую защиту государственной тайны, что создает устойчивую основу для формирования международных обязательств [4].

Значимость защиты государственной тайны не ограничивается рамками одного государства. Она является совместной задачей, решаемой на уровне международных организаций, таких как Организация Договора о коллективной безопасности (ОДКБ). Эти организации создают платформу для обсуждения и разработки

совместных стратегий по охране конфиденциальной информации [3]. Важно, чтобы каждая страна участвовала в этом процессе, учитывая свои национальные интересы и международные обязательства.

Таким образом, международные соглашения о защите государственной тайны способствуют не только укреплению безопасности каждой страны, но и обеспечению стабильности в глобальном масштабе. Участие государств в таких соглашениях позволяет более эффективно реагировать на новые вызовы и угрозы, обеспечивая надежную защиту конфиденциальной информации и предотвращая ее несанкционированное распространение.

Россия активно участвует в международном сотрудничестве по защите государственной тайны, что обусловлено необходимостью обеспечить национальную безопасность и защиту стратегически важных данных. Основными рамками такого взаимодействия служат как двусторонние, так и многосторонние соглашения, направленные на предотвращение утечек информации и обмена лучшими практиками по ее защите. Законодательные акты, такие как Закон РФ «О государственной тайне», регламентируют правила определения, классификации и охраны секретной информации [4].

Важная роль в этой системе отведена правительству и специализированным службам, таким как Федеральная служба безопасности и Служба внешней разведки. Эти органы обладают полномочиями не только для задержания и расследования преступлений в сфере защиты государственной тайны, но и для координации совместных действий на международной арене. Правительство обеспечивает единую политику в этой области, что позволяет России выстраивать эффективные механизмы защиты [3].

Существуют и вызовы, требующие дополнительного сотрудничества. Киберугрозы и современные технологии требуют совместных усилий для разработки новых методов защиты секретной информации. Участие России в киберинициативах и программах безопасности данных подчеркивает её стремление бороться с мошенничеством и утечками информации, что в свою очередь базируется на международных стандартах и совместных разработках с партнерами.

Данные меры позволяют обеспечить не только поддержку внутренней правовой системы России, но и укрепить ее международные позиции как надежного партнёра в области безопасности и защиты государственного секрета.

Сравнительный анализ правовых систем показывает, что большинство стран имеют аналогичные механизмы защиты государственной тайны, однако последние события подчеркивают необходимость пересмотра и адаптации этих механизмов к современным условиям. Например, многие государства уже начали процесс пересмотра эффективных методов, включая улучшение процедур допуска к секретной информации и контроль за ее обращением [4]. Примеры успешного сотрудничества между странами становятся важным аспектом для разработки совместной правовой базы.

К тому же успешное международное сотрудничество в данной сфере зависит от налаживания эффективных каналов обмена информацией и опыта между странами. Формирование единого международного правового пространства в области защиты государственной тайны может значительно упростить взаимодействие государств и повысить устойчивость к современным угрозам [1]. По мере развития новых вызовов важно осуществлять мониторинг и адаптацию существующих норм для обеспечения безопасности в мировом контексте.

Таким образом, государственная тайна требует комплексных мер защиты, включая правовые инструменты, технические средства и международное сотрудничество. В условиях динамично меняющегося мира, государствам необходимо сохранять гибкость и готовность к изменениям для обеспечения своей безопасности и защиты национальных интересов.

Современные условия международной безопасности и глобализации требуют повышения уровня защиты государственной тайны и активизации межгосударственного сотрудничества в этой области. Защита государственной тайны становится важным аспектом политической стабильности и безопасности стран, поскольку утечки секретной информации могут подорвать доверие между государствами и угрожать их национальным интересам. В этом контексте особое значение приобретают правовые и организационные меры, направленные на защиту засекреченных данных.

Соглашения между государствами о защите информации остаются основным инструментом, обеспечивающим совместимость на уровне национального законодательства. Эти соглашения касаются не только передачи

данных, но и определения четких рамок для работы с конфиденциальной информацией. По данным экспертов, успешное сотрудничество требует комплексного подхода, включающего не только правовые аспекты, но и создание единой системы стандартов, обеспечивающих защиту государственной тайны между странами-партнерами [1].

К совместным усилиям также требуется относиться с должным вниманием, поскольку различия в правовых системах могут создавать сложности при реализации соглашений. Необходимость учитывать культурные и правовые особенности разных стран становится важным фактором в процессе формулирования международных норм и стандартов, которые будут применяться при работе с государственной тайной [2].

Совместные исследования и инициативы в области безопасности становятся основой для формирования общих стратегий защиты. Обмен информацией о новых вызовах, таких как киберугрозы, открыл новые горизонты для сотрудничества. Участие в многосторонних форумах и создание специализированных рабочих групп на международных площадках поможет объединить усилия и ресурсы для создания эффективной системы защиты государственной тайны на глобальном уровне.

В условиях глобализации и стремительного развития технологий, вопросы защиты государственной тайны становятся все более актуальными. Государственная тайна представляет собой важный элемент национальной безопасности, и ее утечка может иметь серьезные последствия как для отдельных государств, так и для международной стабильности в целом. В данной работе мы рассмотрели ключевые аспекты международного сотрудничества в области защиты государственной тайны, а также правовые и организационные механизмы, которые используются для обеспечения конфиденциальности информации.

Значение государственной тайны в международных отношениях невозможно переоценить. Она служит основой для защиты стратегических интересов государств, а также для поддержания доверия между ними. В условиях, когда информация становится одним из главных ресурсов, ее защита требует комплексного подхода, включающего как правовые, так и организационные меры. Правовые основы защиты государственной тайны включают в себя международные соглашения, национальные законы и нормативные акты, которые регулируют порядок доступа к конфиденциальной информации и ее использование.

Организационные механизмы защиты государственной тайны также играют важную роль. Они включают в себя создание специализированных органов, ответственных за защиту информации, а также разработку и внедрение современных технологий, способствующих обеспечению безопасности данных. Важным аспектом является сотрудничество между государствами, которое позволяет обмениваться опытом и лучшими практиками в области защиты государственной тайны. Соглашения о сотрудничестве, заключаемые между государствами, направлены на минимизацию рисков несанкционированного доступа к важной информации и создание единой системы защиты.

Роль России в международном сотрудничестве по защите государственной тайны также заслуживает особого внимания. Россия активно участвует в разработке международных стандартов и соглашений, направленных на защиту конфиденциальной информации. В условиях современных вызовов, таких как киберугрозы и терроризм, Россия стремится укрепить свои позиции на международной арене, предлагая новые механизмы сотрудничества и совместные инициативы.

Современные вызовы в области защиты государственной тайны требуют от государств гибкости и готовности к адаптации к новым условиям. Увеличение числа кибератак, развитие технологий шифрования и утечек информации ставят перед государствами новые задачи. Важно не только реагировать на эти вызовы, но и предвидеть их, разрабатывая проактивные меры защиты.

Перспективы развития международного сотрудничества в области защиты государственной тайны выглядят многообещающими. Углубление интеграции между государствами, обмен информацией и совместные проекты могут значительно повысить уровень безопасности. Важно, чтобы государства осознали необходимость совместных усилий в этой области, что позволит не только защитить свои интересы, но и обеспечить стабильность в международных отношениях.

Таким образом, международное сотрудничество в области защиты государственной тайны является важным аспектом обеспечения безопасности в условиях глобализации. Эффективная защита конфиденциальной

информации требует комплексного подхода, включающего правовые, организационные и технологические меры. Важно, чтобы государства продолжали развивать свои механизмы защиты и активно сотрудничали друг с другом, что позволит минимизировать риски и обеспечить безопасность на международной арене.

Литература

1. Государственная тайна – Википедия [Электронный ресурс] // web.archive.org – Режим доступа: https://web.archive.org/web/20211025150624/https://ru.wikipedia.org/wiki/государственная_тайна.

2. Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.08.2024) ...: СудАкт.ру [Электронный ресурс] // sudact.ru – Режим доступа: https://sudact.ru/law/zakon-rf-ot-21071993-n-5485-1-s/.

3. Обеспечение защиты государственной тайны [Электронный ресурс] // is.astral.ru – Режим доступа: https://is.astral.ru/services/zashchita-informatsii/zashchita-gosudarstvennoy-tayny/.

4. Соглашение о защите секретной... – Контур.Норматив [Электронный ресурс] // normativ.kontur.ru – Режим доступа: https://normativ.kontur.ru/document?moduleid=1&documentid=243966.

LUTENKO Evgeny Nikolaevich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

MOHIREV Konstantin Pavlovich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

POPOV Yuri Leonidovich
Candidate of Historical Sciences, Associate Professor, Professor,
Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

INTERNATIONAL COOPERATION IN THE FIELD OF PROTECTION OF STATE SECRETS

Abstract. *The paper will consider the importance of state secrets in international relations. We will look at international agreements and conventions that regulate the protection of confidential information, as well as Russia's role in international cooperation on the protection of state secrets.*

Keywords: *state secret, international relations, agreements, protection, law.*

РОМИН Сергей Александрович
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

КОЗЕЛОВ Владислав Алексеевич
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ПОПОВ Юрий Леонидович
кандидат исторических наук, доцент, профессор,
Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Челябинск

ОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ МОБИЛЬНОЙ СВЯЗИ В ЗОНЕ БОЕВЫХ ДЕЙСТВИЙ

Аннотация. *Данная работа направлена на всесторонний анализ рисков, связанных с использованием мобильной связи в условиях боевых действий, и на выработку практических рекомендаций, которые помогут избежать трагических последствий и повысить уровень безопасности военнослужащих.*

Ключевые слова: *мобильная связь, сотовый телефон, боевые действия, утечка информации, защита, местоположение.*

Современные технологии, в частности мобильная связь, стали неотъемлемой частью нашей повседневной жизни. Однако в условиях боевых действий использование мобильных устройств может представлять собой серьезную угрозу как для военнослужащих, так и для выполнения поставленных задач.

Актуальность данной темы обусловлена тем, что в последние годы наблюдается рост числа конфликтов, где мобильная связь используется как для координации действий, так и для обмена информацией. Однако, несмотря на очевидные преимущества, такие как возможность быстрой связи и получения актуальных данных, существует множество рисков, связанных с раскрытием местоположения военнослужащих и утечкой важной информации. В условиях боевых действий, где каждая секунда может иметь решающее значение, осознание этих рисков становится критически важным.

Мобильная связь в условиях боевых действий открывает ряд уязвимых мест для военнослужащих, что в значительной степени усложняет выполнение поставленных задач и увеличивает риски. Подключенные к сети смартфоны способны передавать данные о местоположении, что может помочь противнику в определении координат. Расстояние, на котором смартфоны могут поддерживать связь с базовыми станциями, варьируется от 3 км в городских условиях и до 7 км на открытой местности, что увеличивает вероятность их обнаружения в зоне боевых действий [1].

Специалисты подчеркивают, что не только военнослужащие, но и гражданские лица, находящиеся в зоне конфликта, могут стать жертвами утечек информации. Следовательно, каждый участник боевых действий должен быть осведомлен об опасностях, связанных с использованием смартфонов. Уязвимость устройств к слежке и перехвату информации делает соблюдение осторожности обязательным [1].

Использование мобильной связи в зоне боевых действий требует глубокого понимания технических аспектов, поскольку от этого зависит не только возможность оперативной связи, но и безопасность личного состава. Мобильные устройства, несмотря на их распространенность, не всегда подходят для использования в условиях активных боевых действий. Поэтому необходимо принимать во внимание

специфические условия, возможные атаки противника и методы защиты информации.

Для начала стоит обратить внимание на выбор смартфона. Устройства, пригодные для боевых условий, должны иметь серьезные технические характеристики, такие как высокая степень защиты данных и возможность работы в сложных условиях. Это означает, что к выбору должны применяться критерии, позволяющие избежать несанкционированного доступа к важной информации. Например, использование зерноподобного шифрования и применение криптографических методов являются необходимыми мерами в современных реалиях боевых действий [1].

На фронте мобильная связь может сохраняться до тех пор, пока не произойдет повреждение инфраструктуры или системы. Однако важно осознавать, что на расстоянии до 10 км от противника использование мобильных устройств должно быть минимизировано или вовсе ограничено, а на большем расстоянии не рекомендуется использовать их группами [2]. В случае воздействия подставных базовых станций противника нужно менять SIM-карты, чтобы избежать подслушивания и других форм вмешательства.

Использование мобильной связи в зоне боевых действий связано не только с техническими и практическими аспектами, но и с серьезными психологическими последствиями. Психологическая осведомленность военнослужащих о возможных рисках и угрозах, связанных с использованием мобильных устройств, может существенно влиять на их поведение в условиях конфликта. В этом контексте важно понять, как осведомленность о рисках может изменить подход к использованию мобильных телефонов.

Одним из главных факторов является необходимость скрытности в общении. Узнавая о том, что использование мобильных телефонов может привести к перехвату информации врагом, многие солдаты начинают действовать более осторожно. Исследования показывают, что даже осознание возможности обнаружения может вызвать увеличение уровня тревожности и стресса, что в свою очередь может повлиять на принятие решений в критических ситуациях [2]. Этот краткий переход от осведомленности к несознательному самоограничению создает двусмысленное положение: с одной стороны, мобильная связь может оказать реальную помощь в координации действий, а с другой – стать причиной уязвимости.

Также стоит отметить, что использование мобильных устройств часто связано с желанием поддерживать связь с семьей и друзьями на гражданской стороне. Однако эта необходимость также может создать дополнительные психологические нагрузки, придавая ситуации больше эмоционального контекста. Солдаты, постоянно думающие о своих близких, могут испытывать дополнительные стрессы, что также влияет на их моральное состояние и реакцию в боевых условиях. Мобильные устройства становятся не только средством связи, но и источником постоянного беспокойства и волнения [2].

Таким образом, осведомленность о рисках, связанных с мобильной связью, не только вызывает добавление психологической нагрузки, но и формирует определенные структуры поведения, ставящие под угрозу как индивидуальную безопасность, так и общую эффективность военных операций.

Опасность использования мобильной связи в зоне боевых действий привлекает внимание экспертов, которые считают, что мобильные телефоны могут стать маяками, указывающими на местоположение военнослужащих.

Одной из рекомендаций экспертов является отказ от использования гражданских мобильных операторов. Исследования показывают, что даже с шифрованием открытая связь может быть подвержена сканированию и вмешательству, что опасно в условиях конфликта. Вместо этого предлагается создание автономных мобильных операторов, которые обеспечат более высокий уровень защиты и снизят риски утечки информации [3].

Необходимо отметить, что существует возможность подавления связи противником на радиостанциях, что еще больше усугубляет ситуацию. В современных боевых условиях мобильные устройства могут стать мишенью для кибератак и электронных средств радиоэлектронной борьбы [1]. Эксперты согласны с тем, что стратегический подход к обеспечению безопасности мобильной связи критически важен для сохранения жизни и здоровья военных личностей в условиях активных боевых действий.

Ситуация усугубляется наличием шпионских программ на мобильных устройствах, которые могут собирать и передавать личные данные жертв. В условиях конфликта, когда информация может передаваться через смартфоны, такие утечки становятся особенно опасными. Одним из недавних случаев является утечка 140 миллионов уникальных номеров и 46 миллионов электронных адресов в России, которая произошла в первой половине 2024 года. Это событие показало, что рынок утечек данных продолжает расти, особенно в сегментах электронной коммерции и финансов [3].

Проблема усугубляется тотальным распространением услуг связи и растущей зависимостью от мобильных технологий. Переход на удаленную работу создал новые риски, так как часть утечек переместилась в «сезонные зоны», где уровень контроля за данными может снижаться [3]. Мобильные операторы фактически признали, что прежде они не придавали должного значения вопросу безопасности данных, и это создает дополнительные риски для военных и других пользователей.

Безопасность мобильной связи в условиях боевых действий требует внимательного изучения существующих рисков и внесения изменений в подход к эксплуатации технологий. Необходимо разработать новые стратегии защиты информации и регулярно обновлять меры контроля, чтобы минимизировать угрозы от утечек данных.

Контроль за использованием мобильной связи в армии включает в себя несколько ключевых методов, направленных на минимизацию рисков и обеспечение безопасности. Запрет на использование сотовых телефонов и радиопередающих устройств на территории воинских частей установлен приказом Министерства обороны России, что направлено на защиту информации и личного состава [4]. Эта мера предназначена для предотвращения утечек данных и защиты от возможного врага, который может воспользоваться мобильными устройствами для получения информации.

Регламентация доступа к информации составляет ещё один аспект контроля. Военнослужащим запрещают раскрывать свои личные данные, информацию о других военнослужащих и данные о местонахождении частей, что является критически важным в условиях боевых действий [4]. Кроме того, действуют ограничения на использование интернет-сервисов, направленные на недопущение распространения аудио и видео материалов, а также геолокационных данных, что значительно уменьшает вероятность раскрытия позиций и планов армии.

Для облегчения связи в условиях боевых действий организуются мобильные переговорные пункты. Эти пункты помогают не только обеспечить связь, но и осуществлять контроль за ее использованием, что позволяет контролировать информацию, передаваемую между военнослужащими [4]. Разработка и применение специализированных технических средств контроля над мобильной связью также в значительной степени повышают уровень безопасности.

Каждый командир части устанавливает свои правила, основываясь на текущих приказах и обстоятельствах, чтобы сохранить режим секретности и минимизировать риски утечки информации. Эти меры являются частью построенной системы, направленной на защиту от угроз, которые могут возникнуть в условиях активных боевых действий. Конечная цель всех этих усилий – создать безопасное пространство для выполнения боевых задач и защитить личный состав от воздействия внешних факторов.

В заключение данной работы следует подчеркнуть, что использование мобильной связи в зоне боевых действий представляет собой многогранную проблему, требующую комплексного подхода к ее решению. Риски, связанные с раскрытием местоположения военных и утечкой информации, становятся особенно актуальными в условиях современных конфликтов, где информация может стать решающим фактором в исходе боевых действий. Технические аспекты функционирования мобильных устройств в боевой обстановке показывают, что даже самые современные технологии не могут гарантировать полную безопасность. Передача радиосигналов, даже в зашифрованном виде, может быть перехвачена противником, что создает угрозу для жизни и здоровья военнослужащих.

Психологические аспекты также играют важную роль в использовании мобильной связи. Осведомленность бойцов о потенциальных угрозах, связанных с использованием мобильных устройств, может значительно снизить риски. Однако, как показывает практика,

многие мобилизованные не имеют достаточной информации о том, как правильно использовать мобильные устройства в условиях боевых действий. Это подчеркивает необходимость проведения регулярных обучающих мероприятий и тренингов, направленных на повышение уровня информированности военнослужащих.

Мнения экспертов подтверждают, что недостаток осведомленности о рисках может привести к трагическим последствиям. Важно учитывать, что в условиях боевых действий каждая мелочь может иметь критическое значение, и игнорирование рекомендаций по безопасному использованию мобильной связи может обернуться серьезными потерями. Анализ случаев утечек информации из-за использования мобильной связи демонстрирует, что даже незначительная ошибка может привести к раскрытию стратегически важной информации, что в свою очередь может поставить под угрозу не только жизнь отдельных военнослужащих, но и целых подразделений.

Методы контроля за использованием мобильной связи в армии должны быть многоуровневыми и включать как технические, так и организационные меры. Это может включать в себя запрет на использование мобильных устройств в определенных зонах, а также внедрение систем мониторинга и анализа трафика. Рекомендации по безопасному использованию мобильной связи в боевых условиях должны основываться на принципах минимизации рисков и повышения уровня безопасности. Важно, чтобы военнослужащие понимали, что соблюдение этих рекомендаций не является лишь формальностью, а жизненно важной необходимостью.

Таким образом, работа подчеркивает, что использование мобильной связи в зоне боевых действий требует внимательного и ответственного подхода. Необходимость строгого контроля и повышения уровня осведомленности среди военнослужащих о рисках, связанных с мобильной связью, является ключевым аспектом, который может существенно повысить безопасность и эффективность выполнения боевых задач. В условиях современного конфликта, где информация становится одним из главных ресурсов, важно не только использовать мобильные технологии, но и делать это с умом, осознавая все возможные последствия.

Литература

1. Почему нельзя использовать мобильные телефоны в зоне… [Электронный ресурс] // nikatv.ru – Режим доступа: https://nikatv.ru/news/obshestvo/pochemu-nelzya-ispolzovat-mobilnye-telefony-v-zone-boevyh-deystviy.

2. Оперативная военная радиосвязь: современные мобильные… [Электронный ресурс] // radiosale.ru – Режим доступа: https://radiosale.ru/stati/sredstva-voennoy-radiosvyazi/.

3. Самая критическая проблема наших Вооруженных Сил в СВО… [Электронный ресурс] // topwar.ru – Режим доступа: https://topwar.ru/219980-samaja-kriticheskaja-problema-nashih-vooruzhennyh-sil-v-svo-svjaz.html.

4. Тактико-специальная подготовка. Лекция 5: Органы и пункты… [Электронный ресурс] // www.voenobr.ru – Режим доступа: https://www.voenobr.ru/uchmaterial/lections/136-tsp5?showall=1.

ROMIN Sergey Alexandrovich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

KOZELOV Vladislav Alekseevich
Cadet, Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

POPOV Yuri Leonidovich
Candidate of Historical Sciences, Associate Professor, Professor,
Military Training and Scientific Center of the Air Force
"Military Air Academy named after Professor N. E. Zhukovsky and Yu.A. Gagarin",
Russia, Chelyabinsk

THE DANGER OF USING MOBILE COMMUNICATIONS IN A COMBAT ZONE

Abstract. *This work is aimed at a comprehensive analysis of the risks associated with the use of mobile communications in combat conditions, and at developing practical recommendations that will help avoid tragic consequences and improve the safety of military personnel.*

Keywords: *mobile communications, cell phone, military operations, information leakage, protection, location.*

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

АЛИЕВ Фарид Худаяр оглы
магистрант, Азербайджанский государственный университет нефти и промышленности, Азербайджан, г. Баку

ТЕСТИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЙ

Аннотация. *В современном мире веб-приложения стали неотъемлемой частью повседневной жизни. От простых сайтов до сложных онлайн-платформ – все они требуют высокого уровня надежности, производительности и безопасности. Тестирование веб-приложений играет ключевую роль в обеспечении качества программного обеспечения. В данной статье рассматриваются основные виды тестирования веб-приложений, такие как функциональное, нагрузочное, пользовательское, кроссбраузерное и тестирование безопасности. Также описаны популярные инструменты и подходы, применяемые в индустрии для автоматизации процессов тестирования. Цель статьи – систематизировать знания о тестировании веб-приложений и подчеркнуть его значимость на всех этапах жизненного цикла программного обеспечения.*

Ключевые слова: *веб-приложения, тестирование, функциональное тестирование, автоматизация, Selenium, Postman, JMeter, производительность, баги, качество.*

Введение

С каждым годом растет количество пользователей, активно использующих веб-приложения для решения различных задач – от общения и покупок до ведения бизнеса и взаимодействия с государственными структурами. Веб-приложения стали критически важными элементами цифровой инфраструктуры, и их отказ или некорректная работа могут привести к серьезным последствиям – от потери репутации до значительных финансовых убытков.

В этих условиях тестирование веб-приложений приобретает особую актуальность. Оно позволяет своевременно обнаруживать ошибки, предотвращать уязвимости и обеспечивать стабильную работу системы под различными нагрузками и в разных условиях эксплуатации. Несмотря на активное развитие технологий и внедрение DevOps-подходов, тестирование остается неотъемлемой частью процесса разработки.

В данной статье будет рассмотрено, какие виды тестирования применяются к веб-приложениям, какие инструменты наиболее популярны среди специалистов, а так же как грамотно организовать процесс тестирования для достижения наилучшего результата.

Тестирование веб-приложений

Веб-приложение – это программа, к которой пользователь получает доступ через веб-браузер по сети. Оно может быть реализовано в различных архитектурных стилях, от традиционного клиент-серверного до современных SPA (Single Page Application). В отличие от настольных программ, веб-приложения не требуют установки и часто обслуживают тысячи пользователей одновременно, что предъявляет особые требования к качеству.

Цели и задачи тестирования веб-приложений

Основная цель тестирования – убедиться, что веб-приложение работает корректно, стабильно и безопасно. Среди задач:

- выявление и устранение ошибок;
- проверка соответствия требованиям;
- обеспечение совместимости с различными браузерами и устройствами;
- проверка производительности под нагрузкой;
- выявление уязвимостей.

Виды тестирования веб-приложений

1. **Функциональное тестирование**. Оценивает, насколько правильно реализованы функции приложения согласно требованиям. Проверяются сценарии входа, регистрация, формы, корзины, фильтры и т. д.

2. Нагрузочное тестирование. Определяет, как система справляется с высоким числом пользователей, большим объемом запросов и данных. Это важно для масштабируемости.

3. Кроссбраузерное тестирование. Обеспечивает корректное отображение и функционирование приложения в разных браузерах (Chrome, Firefox, Safari, Edge и др.) и на разных устройствах.

4. UI/UX тестирование. Проверка удобства интерфейса, юзабилити, отклика на действия пользователя. Помогает выявить недостатки, мешающие комфортному взаимодействию.

5. Тестирование безопасности. Проверка защиты от XSS, SQL-инъекций, утечек данных. Особо важно для приложений, обрабатывающих персональные данные или финансовую информацию.

6. Регрессионное тестирование. После каждого обновления или фикса багов проверяется, что ранее работающие функции не были нарушены.

Этапы тестирования

Процесс тестирования веб-приложений включает следующие шаги:

1. Анализ требований – понимание, что должно быть протестировано.
2. Разработка тест-кейсов и чек-листов – составление сценариев тестирования.
3. Выполнение тестов – ручное или автоматизированное тестирование.
4. Фиксация и отслеживание багов – создание баг-репортов.
5. Ретест – проверка устранения дефектов.
6. Регресс – проверка, не нарушилась ли работа других функций.
7. Отчетность – составление отчетов по итогам тестирования.

Инструменты тестирования

Сегодня существует множество инструментов, которые значительно облегчают тестирование:

- **Selenium** – фреймворк для автоматизации UI-тестирования браузеров.
- **Postman** – удобен для ручного и автоматизированного тестирования API.
- **JMeter** – используется для нагрузочного и стресс-тестирования.
- **BrowserStack / Sauce Labs** – позволяют тестировать веб-приложения на разных браузерах и устройствах онлайн.
- **Bugzilla, Jira, TestRail** – системы для управления тестированием и отслеживания багов.
- **Cypress, Playwright** – современные инструменты автоматизации, популярные среди frontend-разработчиков.

Заключение

Качество веб-приложения напрямую влияет на восприятие компании пользователями, уровень доверия и, как следствие, доход. Ошибки в интерфейсе, сбои при высокой нагрузке, утечки данных – всё это можно предотвратить грамотным тестированием.

Тестирование веб-приложений – это не просто поиск багов, а системный подход к обеспечению надежности и стабильности продукта. Использование разнообразных видов тестирования позволяет выявлять не только технические, но и логические ошибки. Автоматизация тестирования помогает ускорить выпуск новых версий и минимизировать человеческий фактор. Таким образом, тестирование веб-приложений – это важнейший этап жизненного цикла, который требует внимания, системности и профессионального подхода.

Литература

1. Савин С.А. – Тестирование DOT COM, или Пособие по жестокому обращению с багами. – СПб.: БХВ-Петербург, 2007.
2. Канер С., Фолк Дж., Нгуен Х. – Тестирование программного обеспечения. – М.: Вильямс, 2001.
3. R. Black – Managing the Testing Process. – Wiley, 2009.
4. Официальный сайт Selenium: https://www.selenium.dev/.
5. Документация Postman: https://learning.postman.com/.
6. Apache JMeter: https://jmeter.apache.org/.

ALIEV Farid Khudayar oglu
Master's Student, Azerbaijan State University of Petroleum and Industry,
Azerbaijan, Baku

TESTING WEB APPLICATIONS

Abstract. *In today's world, web applications have become an integral part of everyday life. From simple websites to complex online platforms, they all require a high level of reliability, performance, and security. Web application testing plays a key role in ensuring software quality. This article discusses the main types of web application testing, such as functional, load, user, cross-browser, and security testing. It also describes popular tools and approaches used in the industry to automate testing processes. The purpose of the article is to systematize knowledge about web application testing and emphasize its importance at all stages of the vital software cycle.*

Keywords: *web applications, testing, functional testing, automation, Selenium, Postman, JMeter, performance, bugs, quality.*

БУХЕНСКИЙ Дмитрий
Senior Project manager in the IT,
Kanda Software, США, Калифорния, г. Сан-Хосе

ОБЛАЧНЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ ПРОЕКТАМИ: ПРЕИМУЩЕСТВА И ВЫЗОВЫ

Аннотация. *В статье рассматривается влияние облачных технологий на управление проектами в условиях цифровой трансформации бизнеса. Авторы подчеркивают, что облачные решения способствуют повышению мобильности, гибкости, прозрачности и масштабируемости проектной деятельности. Приводятся практические примеры использования таких сервисов, как Trello, Jira, Dropbox и AWS, демонстрирующие положительное влияние облачных инструментов на эффективность работы команд.*

Ключевые слова: *облачные технологии, управление проектами, цифровая трансформация, SaaS, проджект-менеджмент, безопасность данных, масштабируемость, Jira, Trello, AWS, гибкость, мобильность, эффективность команд, интеграция систем, риск-менеджмент.*

С развитием технологий и изменением условий работы компаний, облачные решения становятся важным элементом в управлении проектами. Использование облачных технологий позволяет значительно улучшить эффективность процессов, повысить гибкость и масштабируемость. Однако, несмотря на многочисленные преимущества, внедрение облачных решений в управление проектами также сопряжено с рядом вызовов. В этой статье мы рассмотрим, как облачные технологии влияют на управление проектами, а также какие преимущества и трудности с ними связаны. Мы также рассмотрим примеры из практики и предложим рекомендации для проджект-менеджеров, которые помогут эффективно интегрировать облачные решения в свои проекты.

Преимущества облачных технологий в управлении проектами

Доступность и мобильность

Одним из ключевых преимуществ облачных технологий является доступность и мобильность. Работая с облачными инструментами, проектные команды могут иметь доступ к данным и ресурсам проекта в любой точке мира и в любое время. Это особенно важно для распределенных команд и сотрудников, работающих удаленно.

Пример из практики: Компания Trello использует облачные решения для управления задачами, что позволяет командам из разных уголков мира совместно работать над проектами, следить за прогрессом и оперативно вносить изменения. Согласно исследованию Forrester, 72% компаний, использующих облачные инструменты для совместной работы, заявляют, что это улучшило продуктивность и взаимодействие между командами.

Рекомендация:

Применяйте облачные инструменты для улучшения взаимодействия между командами, особенно если ваши сотрудники работают в разных часовых поясах или удаленно. Выбирайте решения с возможностью интеграции с другими сервисами, такими как Slack или Microsoft Teams, чтобы улучшить обмен информацией. Использование таких инструментов значительно улучшает коммуникацию, делая процесс работы более прозрачным и упрощая решение проблем на всех уровнях.

Снижение затрат на инфраструктуру

Облачные технологии позволяют существенно снизить затраты на поддержку и обновление физической инфраструктуры. Вместо покупки дорогих серверов и другого оборудования, компании могут арендовать облачные ресурсы на условиях «pay-as-you-go», что позволяет гибко масштабировать расходы в зависимости от потребностей.

Пример из практики:

Компания Netflix активно использует облачные технологии, в частности Amazon Web Services (AWS), для обеспечения масштабируемости и высокой доступности своих сервисов. Переход на облачную инфраструктуру позволил Netflix значительно снизить капитальные затраты и обеспечить бесперебойную работу на глобальном уровне.

Рекомендация:

Для стартапов и компаний с ограниченным бюджетом облачные решения позволяют избежать крупных первоначальных затрат на инфраструктуру. Убедитесь, что вы выбираете провайдера, который предлагает прозрачные условия оплаты и возможность масштабирования, чтобы избежать неожиданных расходов. Также следует внимательно следить за использованием ресурсов, чтобы не переплатить за неэффективное использование вычислительных мощностей.

Распространенность использования облачных технологий в разных сферах:

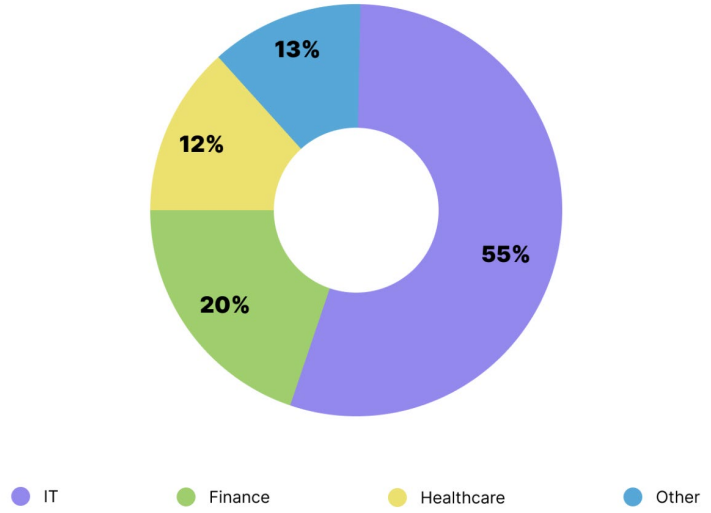

Рис. 1

Гибкость и масштабируемость

Облачные решения обеспечивают «гибкость и масштабируемость», что позволяет проектным менеджерам быстро адаптироваться к изменениям в объеме данных, пользователях или вычислительных мощностях. Когда проект расширяется, можно оперативно увеличить ресурсы, а при необходимости уменьшить их, не затрачивая лишние средства.

Пример из практики:

В компании Dropbox использование облачной платформы позволило быстро масштабировать хранилище данных в зависимости от потребностей проекта и объема информации. Это позволило проектным командам оперативно подстраивать ресурсы под требования бизнеса.

Рекомендация:

При планировании облачной инфраструктуры важно учитывать, что масштабируемость может существенно повлиять на эффективность работы, особенно в периоды высокой нагрузки. Оцените потребности проекта и заранее настройте автоматическое масштабирование, чтобы быть готовыми к изменениям. Также не забывайте проводить регулярные проверки на эффективность использования ресурсов.

Повышение прозрачности и контроля

Использование облачных технологий способствует повышению прозрачности и улучшению контроля над проектами. Облачные инструменты позволяют отслеживать выполнение задач, прогресс проекта и своевременно выявлять возможные отклонения от плана.

Пример из практики:

В одном из крупных ИТ-проектов по разработке системы мониторинга для энергоснабжающей компании мы использовали Jira для отслеживания выполнения задач и оценки состояния проекта. Внедрение облачного решения позволило управлять рисками и оперативно устранять проблемы, поскольку все участники проекта видели актуальные данные и могли быстро реагировать на изменения.

Рекомендация:

Обеспечьте прозрачность всех процессов в проекте с помощью облачных инструментов для управления задачами и мониторинга. Регулярно отслеживайте прогресс и вовремя вносите корректировки, чтобы избежать накопления проблем. Включите в проект план по регулярным ревизиям и встречам для мониторинга состояния.

Влияние облачных технологий на производительность команды:

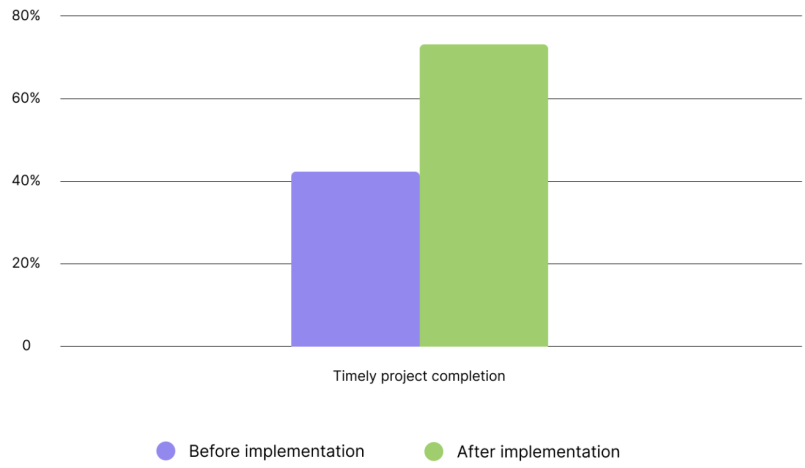

Рис. 2

Вызовы при внедрении облачных технологий в управление проектами

Безопасность данных

Одним из главных вызовов, с которыми сталкиваются компании при использовании облачных технологий, является безопасность данных. Несмотря на то, что облачные провайдеры, такие как Amazon Web Services (AWS) или Microsoft Azure, предлагают высокоуровневую безопасность, ответственность за защиту конфиденциальной информации всё же лежит на организации.

Пример из практики:

В проекте по внедрению облачного хранилища для хранения данных клиентов в финансовой компании мы столкнулись с необходимостью соблюдать строгие требования законодательства о защите данных, такие как GDPR. Для этого мы использовали шифрование данных и ограничение доступа с помощью многофакторной аутентификации.

Рекомендация:

Убедитесь, что облачный провайдер соответствует всем необходимым стандартам безопасности, и внедрите дополнительные меры защиты данных, такие как шифрование и регулярные аудиты. Также важно обучить команду безопасному использованию облачных сервисов. Разработайте четкие политики доступа и защитите критичные данные с помощью многоуровневых систем безопасности.

Зависимость от поставщика облачных услуг

Использование облачных сервисов создает зависимость от конкретного облачного поставщика. Если провайдер сталкивается с техническими проблемами, сбоями или прекращает поддержку своих услуг, это может негативно сказаться на бизнес-процессах.

Пример из практики:

В 2017 году Google Cloud столкнулся с масштабным сбоем, который привел к недоступности ряда сервисов, включая Gmail и YouTube. Это событие подчеркивает важность обеспечения резерва и планирования действий в случае сбоев облачных сервисов.

Рекомендация:

Заключите с поставщиками облачных услуг договоренности о резервных вариантах на случай сбоев, а также обязательно разработайте стратегию восстановления после катастроф и тестируйте её регулярно. Важно также рассматривать мульти-облачные стратегии, чтобы иметь возможность переключаться между различными провайдерами в случае необходимости.

Неполная интеграция с существующими системами

Не всегда облачные технологии легко интегрируются с уже существующими корпоративными системами. Например, если компания использует традиционное локальное ПО, переход на облачные решения может потребовать значительных затрат на интеграцию и обучение персонала.

Пример из практики:

В процессе миграции на облачную систему для управления проектами в одном из моих проектов, мы столкнулись с проблемами интеграции старой ERP-системы с облачным решением для управления задачами. Это потребовало проведения множества тестов и кастомизации интеграционных шлюзов, что увеличило сроки проекта.

Рекомендация:

При планировании перехода на облачные технологии проведите предварительный аудит существующих систем и тщательно спланируйте этапы интеграции. Не забывайте, что потребуется обучение сотрудников для эффективного использования новых решений. Рассматривайте возможность использования промежуточных инструментов для упрощения интеграции.

Проблемы с производительностью

Несмотря на всю гибкость облачных решений, могут возникать проблемы с производительностью, особенно при работе с большими объемами данных или при наличии ограничений в интернет-соединении. Сетевые задержки или сбои в работе облачных серверов могут повлиять на скорость обработки данных и доступность сервисов.

Пример из практики:

В одном из проектов по созданию системы для обработки больших данных мы столкнулись с проблемами производительности на старых серверах, когда объем данных начал значительно увеличиваться. Переход на более мощные облачные платформы помог решить эту проблему, но потребовал дополнительного планирования и оптимизации работы.

Рекомендация:

При выборе облачных сервисов учитывайте не только базовые требования, но и требования к производительности. Работайте с провайдерами, которые могут предложить решения для масштабирования мощности в зависимости от растущих потребностей проекта. Также обязательно учитывайте локальные условия работы сети и проводите стресс-тестирование систем.

Риски и вызовы при внедрении облачных технологий:

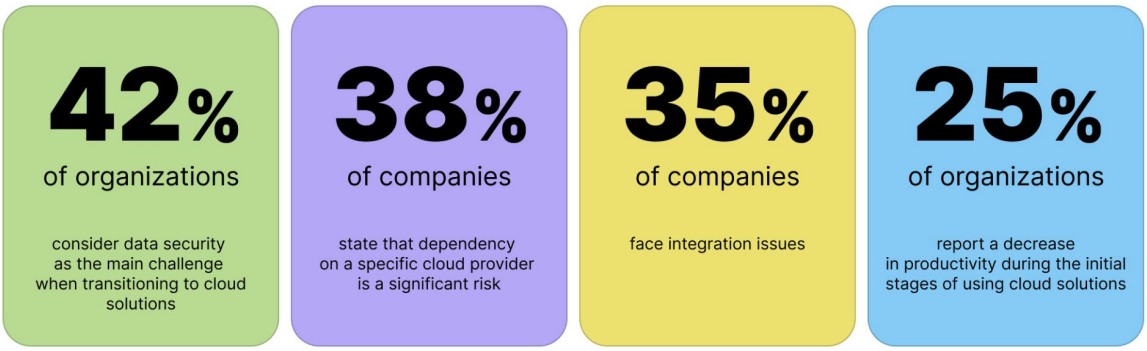

Рис. 3

Заключение

Облачные технологии предоставляют множество преимуществ в управлении проектами, таких как гибкость, доступность и снижение затрат на инфраструктуру. Однако их внедрение сопряжено с рядом вызовов, таких как проблемы безопасности данных, зависимость от поставщика и производительность. Чтобы эффективно использовать облачные решения, проджект-менеджеры должны тщательно планировать переход, учитывать риски и следовать лучшим практикам безопасности. Опыт из практики показывает, что правильное внедрение облачных решений может значительно повысить эффективность проектов, но требует осмотрительности, четкого планирования и постоянного контроля на всех этапах.

Литература

1. The Forrester Wave: Public Cloud Platforms, Q4 2024 – https://www.forrester.com/report/the-forrester-wave-tm-public-cloud-platforms-q4-2024/RES181685.

2. Netflix Architecture on AWS 2024 – https://aws.amazon.com/solutions/case-studies/innovators/netflix/.

3. GDPR compliance for AWS 2025 – https://aws.amazon.com/compliance/gdpr-center/.

4. Google Cloud Outage 2017 – https://www.datacenterknowledge.com/outages/a-history-of-google-cloud-and-data-center-outages.

5. State of Cloud Report 2021 – https://www.flexera.com/about-us/press-center/flexera-releases-2021-state-of-the-cloud-report.

6. Impact of Cloud on Project Management 2020 – https://actionablestrategies.com/wp-content/uploads/2020/05/Impact-of-Cloud-on-Project-Management.pdf.

BUKHENSKY Dmitry
Senior Project manager in the IT,
Kanda Software, USA, California, San Jose

CLOUD TECHNOLOGIES IN PROJECT MANAGEMENT: ADVANTAGES AND CHALLENGES

Abstract. *The article examines the impact of cloud technologies on project management in the context of digital business transformation. The authors emphasize that cloud solutions contribute to increased mobility, flexibility, transparency, and scalability of project activities. Practical examples of using services such as Trello, Jira, Dropbox, and AWS are provided, demonstrating the positive impact of cloud tools on the team's work efficiency.*

Keywords*: cloud technologies, project management, digital transformation, SaaS, data security, scalability, Jira, Trello, AWS, flexibility, mobility, team effectiveness, system integration, risk management.*

ВОДЯНОВ Игнат Николаевич
студент, Московский государственный технологический университет «СТАНКИН»,
Россия, г. Москва

Научный руководитель – доцент кафедры информационных технологий и вычислительных систем Московского государственного технологического университета «СТАНКИН», кандидат технических наук Волкова Ольга Рудольфовна

МЕТОДЫ АНАЛИЗА ТЕКСТОВЫХ ДАННЫХ ДЛЯ ВЫЯВЛЕНИЯ СМЫСЛОВЫХ ПАТТЕРНОВ С ЦЕЛЬЮ УЛУЧШЕНИЯ ВЗАИМОДЕЙСТВИЯ С КЛИЕНТОМ В СИСТЕМЕ OMS

Аннотация. *В статье рассматриваются современные методы анализа текстовых данных, применяемые для выявления смысловых паттернов, и обосновывается их применение для повышения эффективности взаимодействия с клиентами в системах управления заказами (Order Management System, OMS). Основное внимание уделено применению языковых моделей, тематического моделирования, анализа N-грамм и семантических эмбеддингов. Представлены теоретические предпосылки, методологическая база и значимость таких подходов для извлечения релевантной информации, отражающей намерения и потребности клиентов.*

Ключевые слова: *смысловые паттерны, анализ текстов, взаимодействие с клиентами, OMS, тематическое моделирование, RuBERT, BERTopic, N-граммы, эмбеддинги.*

В условиях цифровой трансформации особое значение приобретает интеллектуальный анализ неструктурированных данных, особенно в таких системах, как OMS (Order Management System), которые являются критически важными для оперативного управления заказами, клиентским взаимодействием и логистикой. Интеграция модуля анализа смысловых паттернов в OMS позволяет не только реагировать на входящие обращения, но и предугадывать клиентские потребности, выявлять риски и прогнозировать потенциальные сбои в процессе обслуживания.

Такой подход может быть реализован через архитектуру событийной обработки, в которой каждый фрагмент текста от клиента (например, отзыв, обращение в поддержку, комментарий) становится входным событием для модуля анализа. Далее извлечённые паттерны автоматически сопоставляются с заранее заданными сценариями или правилами, что позволяет системе выдавать предупреждения, генерировать рекомендации для сотрудников или автоматически настраивать параметры взаимодействия с клиентом (например, изменение времени ответа, предложения скидок и др.).

Дополнительным преимуществом внедрения модуля смыслового анализа является возможность представления результатов в виде дашбордов, которые демонстрируют ключевые темы, эмоциональные паттерны и тренды в изменении клиентской обратной связи. Например, если за последние две недели наблюдается рост обращений, содержащих негативную тональность по теме «доставка», это может свидетельствовать о системной проблеме, требующей оперативного вмешательства. Такие аналитические представления становятся неотъемлемой частью процесса принятия решений в клиентских отделах и службах качества.

Современные подходы к анализу больших текстовых данных базируются на применении методов машинного обучения, статистики и лингвистики. Для выявления смысловых паттернов используются как классические статистические методы, так и нейросетевые языковые модели.

Современные подходы к анализу текстовых данных позволяют эффективно выявлять неявные зависимости и ключевые паттерны, которые могут быть использованы для повышения качества обслуживания клиентов. Среди таких методов особое внимание заслуживают тематическое моделирование (например, LDA и BERTopic), а также подходы, основанные на

языковых моделях, таких как RuBERT [1, с. 16-18].

Модель RuBERT – русскоязычная версия трансформера BERT, адаптированная для обработки текстов на русском языке. Она обеспечивает глубокое семантическое представление текста благодаря механизму внимания (attention), учитывающему контекст слов в предложении. Применение RuBERT позволяет выявлять скрытые смыслы и отношения между словами, что критически важно для извлечения смысловых паттернов в пользовательских запросах и сообщениях [3, с. 44-48].

Особую ценность в рамках представленной разработки представляет использование алгоритма HDBSCAN, который позволяет гибко определять плотность кластеров и тем самым эффективно разделять даже слабовыраженные смысловые группы. В отличие от традиционных методов, HDBSCAN способен работать с шумными данными и выявлять структуры, которые сложно поддаются формализации.

BERTopic использует кластеризацию эмбеддингов и тематическое моделирование с извлечением ключевых слов для каждого кластера. Метод позволяет определять скрытые темы в массиве текстов, что помогает сегментировать сообщения клиентов по смысловым признакам. LDA (Latent Dirichlet Allocation) применяет байесовский подход и выявляет латентные темы в текстах, на основе которых можно формировать поведенческие модели клиентов [3, с. 44-48].

Анализ биграмм и триграмм позволяет выявлять часто встречающиеся лексические шаблоны. Расчет PMI (Pointwise Mutual Information) помогает отфильтровывать случайные сочетания слов, выделяя информативные и устойчивые фразы, связанные с конкретными клиентскими проблемами или запросами [2, с. 100-102].

Семантические эмбеддинги (Word2Vec, FastText, BERT) используются для представления слов и предложений в виде числовых векторов, что позволяет измерять семантическую близость и выявлять паттерны в тексте. Такие представления являются входными данными для кластеризации и классификации [1, с. 16-18].

В системах OMS тексты поступают в виде описаний заказов, комментариев к обращениям, чатов и отзывов. Применение описанных методов позволяет: группировать клиентов по смыслу их запросов, выявлять типичные жалобы и предпочтения, формировать шаблоны ответов и прогнозов, оптимизировать маршрутизацию обращений.

Смысловые паттерны, извлеченные из данных, становятся опорными точками для принятия решений: запуск таргетированных акций, автоматическое распределение задач, персонализация коммуникации и пр.

Например, выявление паттернов, связанных с частыми жалобами на задержку заказов или неудобный интерфейс, позволяет оперативно инициировать изменения в логистике или пользовательском интерфейсе. Это делает взаимодействие с системой более отзывчивым к потребностям клиента, повышая уровень доверия и лояльности.

Предложенное решение может быть масштабировано для анализа текстов на других языках и применено в смежных системах – CRM, ERP, Help Desk. Благодаря модульной архитектуре возможно адаптировать алгоритмы под конкретные бизнес-процессы, а также обучать модель на специфических данных организации для повышения точности анализа.

Выявление смысловых паттернов из текстовых данных в OMS представляет собой важный шаг к интеллектуализации взаимодействия с клиентом. Рассмотренные методы обеспечивают многослойный анализ, включая как поверхностные (частотные), так и глубокие семантические уровни обработки текста. Их интеграция в прикладные решения позволяет организациям существенно повысить качество обслуживания и лояльность клиентов.

Литература

1. Томашевская В.С. Использование машинного обучения для распознавания текстовых шаблонов литературных источников / В.С. Томашевская, Ю.В. Старичкова, Д.А. Яковлев. – Текст: непосредственный // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2022. – № 3. – С. 16-18.

2. Краснов Ф.В. Оценка прикладного качества тематических моделей для задач кластеризации / Ф.В. Краснов, Е.Н. Баскакова, И.С. Смазневич. – Текст: непосредственный // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. – 2021. – № 56. – С. 100-102.

3. Разработка и исследование моделей многоклассовых классификаторов для рекомендательной системы подготовки заявок на

портале единой информационной системы в сфере закупок / Я.А. Селиверстов, А.А. Комиссаров, А.А. Лесоводская [и др.]. – Текст: непосредственный // Информатика, телекоммуникации и управление. – 2022. – № 2. – С. 44-48.

VODYANOV Ignat Nikolaevich
Student, Moscow State Technological University "STANKIN", Russia, Moscow

Scientific Advisor – Associate Professor of the Department of Information Technology and Computing Systems at the Moscow State Technological University "STANKIN", Candidate of Technical Sciences Volkova Olga Rudolfovna

METHODS OF TEXT DATA ANALYSIS TO IDENTIFY SEMANTIC PATTERNS IN ORDER TO IMPROVE CUSTOMER INTERACTION IN THE OMS SYSTEM

Abstract. *The article discusses modern methods of text data analysis used to identify semantic patterns, and substantiates their use to improve customer interaction in order Management Systems (OMS). The main focus is on the use of language models, thematic modeling, N-gram analysis, and semantic embeddings. The theoretical background, methodological basis and importance of such approaches for extracting relevant information reflecting the intentions and needs of clients are presented.*

Keywords: *semantic patterns, text analysis, customer interaction, OMS, thematic modeling, RuBERT, BERTopic, N-grams, embeddings.*

ГАЛИН Никита Олегович
студент, МИРЭА – Российский технологический университет, Россия, г. Москва

Научный руководитель – доцент кафедры защиты информации МИРЭА – Российского технологического университета, кандидат технических наук Гуляев Александр Юрьевич

РАЗРАБОТКА УЧЕБНОЙ СИСТЕМЫ ДЛЯ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ПЕРСОНАЛА К АТАКАМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация. *В статье представлена архитектура учебной системы для выявления и предотвращения компрометации сотрудников через атаки социальной инженерии. Проведен анализ основных угроз информационной безопасности, связанных с человеческим фактором. Разработан механизм имитации реальных атак в контролируемой среде с последующим обучением персонала. Предложенная система включает модули фишинговых симуляций, поддельных веб-ресурсов и автоматизированной оценки поведенческих реакций сотрудников.*

Ключевые слова: *информационная безопасность, социальная инженерия, фишинг, человеческий фактор, учебная система, имитация атак.*

В условиях стремительной цифровизации бизнес-процессов проблема обеспечения информационной безопасности приобретает критическое значение для современных организаций. Несмотря на значительные инвестиции в технические средства защиты, статистика кибератак демонстрирует, что более 80% успешных инцидентов связано с человеческим фактором [1, с. 45-52]. Сотрудники организаций остаются наиболее уязвимым звеном в системе информационной безопасности, подверженным воздействию методов социальной инженерии.

Социальная инженерия представляет собой комплекс приемов психологического воздействия, направленных на принуждение человека к совершению действий, нарушающих политику безопасности организации [2]. Основными векторами атак являются фишинг, вишинг, претекстинг и физическое проникновение. Особую опасность представляют таргетированные атаки, использующие персонализированную информацию о сотрудниках и специфике деятельности организации.

Традиционные подходы к обучению персонала, основанные на формальных инструктажах и теоретических семинарах, показывают недостаточную эффективность в формировании устойчивых поведенческих паттернов [3, с. 12-18]. Возникает необходимость разработки практико-ориентированных систем, позволяющих моделировать реальные угрозы в безопасной контролируемой среде.

Проведенный анализ показал, что основными проблемами существующих подходов к обеспечению информационной безопасности являются:

1. **Недостаточная осведомленность персонала** о современных методах социальной инженерии и способах противодействия им.
2. **Отсутствие практических навыков** распознавания и реагирования на потенциальные угрозы в реальных условиях.
3. **Формальный характер обучения**, не учитывающий психологические особенности восприятия угроз.
4. **Отсутствие обратной связи** и индивидуализации процесса обучения.

Анализ нормативно-правовой базы показал, что требования Федерального закона № 152-ФЗ «О персональных данных» и ГОСТ Р 57580.1-2017 предусматривают необходимость обучения персонала и проведения оценки человеческих рисков, что обосновывает актуальность разрабатываемого решения.

Предлагаемая архитектура учебной системы основана на модульном принципе и включает следующие компоненты:

- Модуль генерации сценариев атак – обеспечивает создание реалистичных фишинговых писем и поддельных веб-страниц с

использованием шаблонов, адаптированных под специфику организации.

- Система управления рассылками – реализует автоматизированную отправку тестовых сообщений с учетом ролевой модели и графика обучения.
- Модуль имитации веб-ресурсов – создает поддельные страницы авторизации, максимально приближенные к оригинальным корпоративным сервисам.
- Система мониторинга и аналитики – фиксирует поведенческие реакции сотрудников и формирует детализированные отчеты для анализа уязвимостей.
- Модуль обратной связи – предоставляет персонализированные обучающие материалы сразу после выявления нежелательного поведения.

Взаимодействие компонентов системы представлено в таблице 1.

Таблица 1

Компоненты учебной системы и их функции

Компонент	Основная функция	Технология реализации
Генератор сценариев	Создание реалистичных имитаций атак	Python, Flask, Jinja2
Система рассылки	Автоматизированная отправка писем	smtplib, SQLite/PostgreSQL
Веб-имитатор	Создание поддельных страниц	HTML/CSS/JavaScript
Модуль аналитики	Сбор и анализ поведенческих данных	Python, Pandas, Plotly
Обратная связь	Персонализированное обучение	LMS-интеграция

Механизм функционирования системы

Работа системы осуществляется в несколько этапов:

1. **Планирование кампании** – определение целевой аудитории, типа сценария и временных рамок проведения.
2. **Генерация контента** – создание фишинговых писем и поддельных страниц с использованием корпоративного стиля.
3. **Проведение симуляции** – отправка тестовых сообщений и мониторинг реакций сотрудников.
4. **Анализ результатов** – автоматическое формирование отчетов и выявление уязвимых групп.
5. **Обучение и коррекция** – предоставление целевых обучающих материалов и планирование повторных тестов.

Ключевой особенностью системы является реализация принципа «безопасного провала» – сотрудники, попавшиеся на симуляцию, немедленно получают обучающий контент вместо наказания, что способствует формированию позитивного отношения к процессу обучения.

Результаты тестирования и внедрения

Пилотное внедрение системы было проведено в организации с численностью персонала 150 человек. Результаты представлены в таблице 2.

Таблица 2

Результаты тестирования системы

Показатель	До внедрения	После 3 месяцев	Изменение
Успешность фишинговых атак	45%	12%	-73%
Обращения в ИБ-службу	5%	35%	+600%
Время реакции на подозрительные письма	>24 часа	<2 часов	Значительное улучшение
Общая осведомленность (тестирование)	60%	87%	+27%

Результаты демонстрируют значительное повышение киберустойчивости организации и формирование проактивного отношения сотрудников к вопросам информационной безопасности.

Выводы

В ходе исследования была разработана и апробирована учебная система для повышения устойчивости персонала к атакам социальной инженерии. Основными преимуществами предложенного решения являются:

1. **Практико-ориентированный подход** к обучению, основанный на реальных сценариях угроз.
2. **Автоматизация процессов** планирования, проведения и анализа результатов обучающих кампаний.

3. **Персонализация обучения** с учетом индивидуальных особенностей и уровня подготовки сотрудников.

4. **Интеграция в корпоративные процессы** без нарушения рабочих процессов.

Дальнейшее развитие системы предполагает внедрение машинного обучения для адаптивной генерации сценариев, интеграцию с системами управления инцидентами и расширение спектра моделируемых угроз.

Литература

1. Вопросы кибербезопасности. 2023. № 4. С. 45-52.

2. Молдовян Н.А., Молдовян А.А. Криптография: от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2022. 448 с.

3. Зайцев И.В., Петров А.С. Социальная инженерия в информационной безопасности // Вестник компьютерных и информационных технологий. 2023. № 2. С. 12-18.

4. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Общие положения. М.: Стандартинформ, 2017.

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

GALIN Nikita Olegovich
Student, MIREA – Russian Technological University, Russia, Moscow

Scientific Advisor – Associate Professor of the Department of Information Security at MIREA – Russian Technological University, Candidate of Technical Sciences Gulyaev Alexander Yurievich

DEVELOPMENT OF A TRAINING SYSTEM TO INCREASE STAFF RESILIENCE TO SOCIAL ENGINEERING ATTACKS

Abstract. *The article presents the architecture of a training system for detecting and preventing employee compromise through social engineering attacks. An analysis of the main information security threats related to the human factor was conducted. A mechanism for simulating real attacks in a controlled environment with subsequent staff training has been developed. The proposed system includes modules for phishing simulations, fake web resources and automated assessment of employees' behavioral reactions.*

Keywords: *information security, social engineering, phishing, human factor, training system, attack simulation.*

ЖИЛЕНКОВ Кирилл Максимович
магистрант, Иркутский национальный исследовательский технический университет,
Россия, г. Иркутск

ЖЕЛТОВ Константин Юрьевич
преподаватель, Иркутский национальный исследовательский технический университет,
Россия, г. Иркутск

КОМПЛЕКСНОЕ ИЗУЧЕНИЕ СНА: ОТ ФИЗИОЛОГИИ ДО ТЕХНОЛОГИЙ МОНИТОРИНГА

Аннотация. *В данной статье рассматриваются основные аспекты сна, его физиологические фазы, методы диагностики и роль современных технологий в мониторинге сна. Освещены как традиционные, так и инновационные подходы к изучению сна, включая использование носимых устройств и амбулаторные методы диагностики. Статья предоставляет комплексный обзор текущего состояния исследований в области сна, подчеркивая важность объединения различных методов для достижения наиболее точной и полной оценки сна, подчеркивая тонкости использования существующих аппаратно-программных решений.*

Ключевые слова: *сон, фазы сна, полисомнография, актиграфия, фитнес-трекеры, мониторинг сна, качество сна, здоровье.*

Содержание

Сон является одним из фундаментальных биологических процессов, играющих ключевую роль в поддержании физического и психического здоровья человека. Современные исследования подтверждают, что качество и продолжительность сна оказывают значительное влияние на когнитивные функции, эмоциональное состояние, продуктивность и даже социальные взаимодействия. В данной статье мы рассмотрим основные аспекты сна, включая его фазы, методы диагностики, альтернативные подходы к организации сна и роль технологий в его анализе, стремясь предоставить комплексный обзор текущего состояния исследований в этой области.

В сомнологии существует понятие «Норма качества сна». Национальный фонд сна США (2017) предлагает следующие критерии (табл.).

Таблица

Нормы качества сна

Показатель	Норма	Допустимо для пожилых
Латентность засыпания	⩽15 минут	31–60 минут
Пробуждения (>5 минут)	До 2 раз/ночь	До 3 раз
Время бодрствования после сна	⩽20 минут	31–60 минут
Дневной сон	⩽20 минут (для подростков)	⩽100 минут

Эксперты Американской ассоциации медицины сна рекомендуют взрослым спать не менее 7 часов в сутки для поддержания оптимального здоровья и благополучия.

Сон, как фундаментальный биологический процесс, обладает сложной и хорошо регулируемой структурой, которая включает две основные фазы: медленноволновой сон (NREM) и быстрый сон (REM). Эти фазы чередуются в течение ночи, формируя циклы продолжительностью примерно от 90 до 120 минут, которые повторяются 4–6 раз за ночь в зависимости от индивидуальных особенностей сна человека. Фаза NREM, которая составляет большую часть сна, подразделяется на три стадии: N1, N2 и N3. Первая стадия, N1, является переходной от бодрствования ко сну и занимает около 5% от общего времени сна. Вторая стадия, N2, составляет примерно 45–55% сна и характеризуется более глубоким сном, во

время которого человек становится менее чувствителен к внешним раздражителям. Третья стадия, N3, известная как глубокий или дельта-сон, является самой восстановительной фазой и занимает 15–25% ночного сна. В этот период происходит восстановление физического тела и укрепление иммунной системы. Фаза REM, которая начинается примерно через 90 минут после засыпания, отличается активной работой мозга, похожей на бодрствование. Эта фаза занимает около 20–25% общего времени сна и связана с обработкой эмоций, консолидацией памяти и сновидениями. Во время REM-сна происходит усиление мозговой активности, что способствует обработке информации и укреплению нейронных связей. Нарушения в этих фазах сна могут привести к значительному ухудшению самочувствия, снижению когнитивных функций и увеличению риска развития хронических заболеваний. Недостаток сна, особенно хронический, связан с увеличением вероятности развития сердечно-сосудистых заболеваний, метаболических нарушений, таких как диабет, и психологических расстройств, включая депрессию. С другой стороны, избыточный сон также может быть вредным, ассоциируясь с повышенным риском инсультов и ожирения.

Современные исследования сна сочетают медицинские, психологические и технологические подходы. Полисомнография (ПСГ) остается «золотым стандартом» в исследовании сна. Она регистрирует ЭЭГ, движения глаз, тонус мышц, дыхание и другие параметры. Однако метод требует пребывания пациента в лаборатории, что может вызывать «эффект первой ночи» – искажение данных из-за стресса. Для амбулаторного мониторинга используются, среди прочего, два метода. Первый из них актиграфия – запись активности с помощью акселерометра. Точность этого метода составляет 89–98% у здоровых людей, но снижается у пациентов с расстройствами сна. Второй – это опросники, представляющие субъективную оценку, часто неточную. Например, люди склонны завышать продолжительность сна на 15–20 минут [2].

С развитием технологий носимых устройств, таких как умные часы и фитнес-трекеры, появились новые возможности для самостоятельного анализа сна. Эти устройства активно используются для регистрации движений, пульса и освещенности окружающей среды [1, с. 1538-1557], что позволяет пользователям оценивать различные фазы сна и периоды бодрствования. Однако, несмотря на широкие возможности, алгоритмы фитнес-трекеров имеют свои ограничения. Они могут ошибочно интерпретировать начало и конец сна, а также не учитывать внешние маркеры, такие как выключение света. Это требует от пользователей критического подхода к анализу получаемых данных и, в некоторых случаях, ведения дополнительных личных заметок для точной аннотации результатов. Фитнес-трекеры обычно фиксируют состояния «сон», «бодрствование» и «беспокойный сон» с интервалом в одну минуту. При соблюдении определенных условий, таких как длительность сна более трех часов и надежный контакт сенсора с кожей, устройства способны дифференцировать REM-сон, а также легкие и глубокие стадии сна. Принцип работы фитнес-трекеров основан на использовании акселерометрии и фотоплетизмографии (PPG) непрямой мониторинг температуры тела (STM).

Акселерометры отслеживают активность запястья, предполагая, что отсутствие движений свидетельствует о сне, а активность – о бодрствовании. Однако такой подход имеет свои недостатки: устройство может ошибочно считать состояние покоя без движений за сон или не заметить пробуждения, сопровождаемые минимальной активностью. В то же время акселерометр является основным датчиком в устройствах регистрации сна – актиграфовах, что требует применения дополнительных средств регистрации физиологического состояния, таких как кардиограф, что затрудняет широкое применение данных средств регистрации. С другой стороны, в фитнес-браслетах применяется механизм фотоплетизмографии – измеряет пульс и вариабельность сердечного ритма через световые датчики, что помогает уточнить фазы сна. Например, учащение пульса может указывать на наступление REM-фазы. Тем не менее алгоритмы, используемые устройствами для классификации фаз сна, разработанные компанией Fitbit, основываются на данных о движении и пульсе. Эти алгоритмы могут ошибочно интерпретировать начальные и конечные стадии сна как периоды бодрствования, что влияет на точность расчетов времени засыпания и пробуждения. Отсутствие учета внешних маркеров также ограничивает возможности анализа, делая результаты менее надежными.

Обозначив достоинства и недостатки программно-аппаратных способов исследования сна, был предпринят эксперимент по определению сравнительного качества получаемых данных с фитнес-браслетов (носимых устройств), как альтернативе актиграфам. При построении собственного механизма регистрации времени периодов сна применялся классический метод.

Разрабатываемый механизм регистрации времени периодов сна базируется на классическом подходе к журналированию собственного графика этого сна. При этом было реализовано мобильное приложение, которое регистрирует и агрегирует данные с множества датчиков для их дальнейшей статистической обработки. В сравнении с классическим подходом. Для получения данных о сне применялись встроенные программные API следующих устройств: Fitbit (какой), Honor Band 6, Samsung Galaxy Watch 5. Был использован механизм REST API и протокол авторизированного доступа OAuth 2.0. Данные с фитнес-браслетов агрегировались на сервере, где подвергались статистической обработке с помощью математических библиотек для языка Python.

Для получения токена доступа к API использовались функции, которые реализовывали протокол OAuth 2.0 для предотвращения неавторизованных клиентов и обеспечивали безопасность передачи личных данных. После получения токена доступа, клиенты отправляли запрос на установку соединения защищенного соединения с сервером, используя HTTP методы GET и POST, после чего осуществляли обмен данными.

Например, для получения данных о сне через API Fitbit, использовался параметризованный метод GET для отправки, а затем входящий массив данных преобразовывался к обрабатываемому виду с помощью функции json.loads. Аналогичным образом процедура обмена данными реализована в API WearOS. Минимальные отличия наблюдались в части утилизации API WearOS.

Для обработки персональных данных организована система управления реляционной базой данных под управлением Room и определена схема организации данных в структурированный вид.

Результатом сравнительного анализа точности определения времени начала и окончания периода сна, стали диаграмма, где точками были отмечены случаи, когда носимые устройства показывали время, отличающееся на 10 минут в ту или иную сторону от того, что было в действительности по показаниям из заполняемых вручную журналов испытуемых. Одна из таких диаграмм для одного человека представлена на рисунке. Как можно видеть ошибка не столь существенна в количественном аспекте и наблюдается главным образом в момент позднего отхода ко сну и вероятно, активным или иным выделяющимся поведением испытуемого во время засыпания.

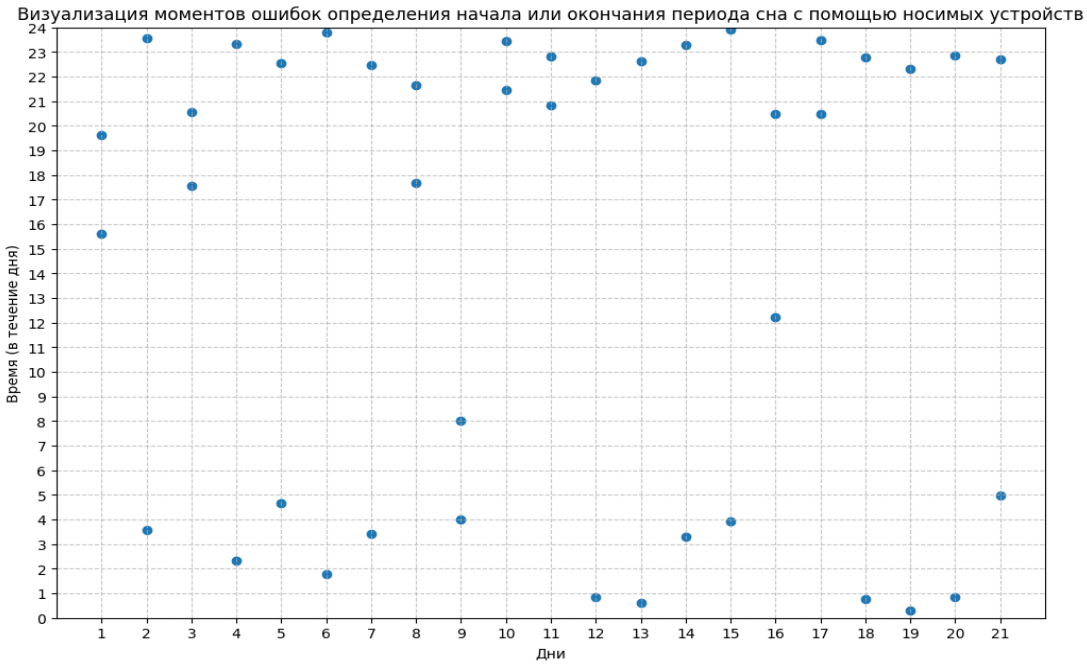

Рис. 1. Диаграмма визуализации моментов отклонения показателей носимых устройств от журналируемого вручную графика

Фитнес-трекеры, несмотря на свои ограничения, всё чаще становятся важным альтернативным инструментом современной медицины и исследований здоровья [3]. Среди ограничивающих факторов, в ходе исследования выявлены: зависимость от заряда батареи, качество непосредственного контакта с кожей пользователя. К тому же производители могут вносить изменения в программное обеспечение устройств без предварительного уведомления, что потенциально может привести к искажению данных в долгосрочных исследованиях. Предлагаемый алгоритм уважительно относится к пользователю и не начинает свою работу по без предварительного согласия с его стороны и предоставления ему условий работы программы, способе и порядке передаче данных.

В заключении следует отметить, что носимые устройства предоставляют уникальную возможность для массового сбора данных о сне населения в естественных условиях. Они позволяют мониторить динамику изменений в качестве сна, что может помочь выявить различные тенденции, например, как стресс или изменения в диете влияют на сон. Использование фитнес-трекеров в сочетании с другими методами, такими как актиграфия или анкетирование, может повысить объективность получаемых данных, позволить совершенствовать алгоритмы обработки показаний [4].

Литература

1. De Zambotti M. [и др.]. Wearable Sleep Technology in Clinical and Research Settings // Medicine & Science in Sports & Exercise. 2019. № 7 (51). С. 1538-1557.

2. Тихомирова О.В. Диагностика и лечение нарушение сна /учебно-методическое пособие / Всероссийский центр экстренной и радиационной медицины им. А.М. Никифорова МЧС России. СПб.: ООО «НПО ПБ АС», 2020. 52 с.

3. Inderkum A.P., Tarokh L. High heritability of adolescent sleep–wake behavior on free, but not school days: a long-term twin study // Sleep. 2018. № 3 (41).

4. Menghini L. [и др.]. A standardized framework for testing the performance of sleep-tracking technology: step-by-step guidelines and open-source code // Sleep. 2021. № 2 (44).

ZHILENKOV Kirill Maksimovich
Master's Student, Irkutsk National Research Technical University, Russia, Irkutsk

ZHELTOV Konstantin Yurievich
Lecturer, Irkutsk National Research Technical University, Russia, Irkutsk

COMPREHENSIVE STUDY OF SLEEP: FROM PHYSIOLOGY TO MONITORING TECHNOLOGIES

Abstract. *This article discusses the main aspects of sleep, its physiological phases, diagnostic methods, and the role of modern technologies in sleep monitoring. Both traditional and innovative approaches to sleep research are highlighted, including the use of wearable devices and outpatient diagnostic methods. The article provides a comprehensive overview of the current state of sleep research, emphasizing the importance of combining various methods to achieve the most accurate and complete sleep assessment, emphasizing the intricacies of using existing hardware and software solutions.*

Keywords*: sleep, sleep phases, polysomnography, actigraphy, fitness trackers, sleep monitoring, sleep quality, health.*

ЛЫГАРЕВ Максим Сергеевич
студент, МИРЭА – Российский технологический университет, Россия, г. Москва

ГУЛЯЕВ Александр Юрьевич
кандидат технических наук, доцент,
МИРЭА – Российский технологический университет, Россия, г. Москва

ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ ЗАЩИЩЕННОЙ СИСТЕМЫ ОБМЕНА СООБЩЕНИЯМИ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙН ТЕХНОЛОГИЙ

Аннотация. *В статье представлена архитектура защищенной системы обмена сообщениями. Была разработана схема взаимодействия компонентов системы. В ходе сравнительного анализа обнаружены недостатки в традиционных системах обмена сообщениями. На основе результатов сделан вывод о необходимости создания спроектированной системы. Это позволит повысить уровень безопасности передачи информации и улучшить эффективность работы.*

Ключевые слова: *информационная безопасность, информация, система обмена сообщениями, архитектура, блокчейн.*

Вводная часть

В современном мире обмен информацией через электронные каналы связи стал неотъемлемой частью как личной, так и деловой коммуникации. Однако с ростом объема передаваемой информации увеличиваются и риски, связанные с её безопасностью. Традиционные централизованные системы обмена сообщениями сталкиваются с рядом проблем, включая уязвимость к атакам типа «человек посередине», риски компрометации ключей шифрования, а также возможность несанкционированного доступа к данным со стороны третьих лиц или даже самих провайдеров услуг.

Блокчейн-технологии, изначально разработанные для обеспечения безопасных и прозрачных финансовых транзакций, предоставляют новые возможности для создания защищенных систем обмена сообщениями. Децентрализованная природа блокчейна, использование криптографических методов и механизмы консенсуса позволяют преодолеть многие недостатки традиционных систем.

Проведем сравнительный анализ централизованных и децентрализованных СОС. Результат представлен в таблице.

Таблица

Сравнительный анализ СОС

Система	Безопасность	Приватность	Масштабируемость	Децентрализация
WhatsApp	Высокая	Средняя	Высокая	Низкая
Telegram	Высокая	Высокая	Очень высокая	Низкая
Signal	Очень высокая	Очень высокая	Средняя	Низкая
Discord	Средняя	Низкая	Очень высокая	Низкая
Matrix	Высокая	Высокая	Средняя	Высокая
Блокчейн-мессенджеры	Очень высокая	Очень высокая	Низкая-Средняя	Очень высокая

Существующие централизованные системы обмена сообщениями предлагают либо высокую безопасность и приватность, либо отличную масштабируемость, но редко сочетают эти качества с децентрализацией.

Учитывая произведенный анализ, было принято решение использовать блокчейн-технологии для работы с метаданными и классическое хранилище для контента для более оптимальной работы.

Основная часть

Архитектура разрабатываемой системы является комплексным решением, интегрирующим современные технологии для обеспечения

безопасного обмена сообщениями. Многоуровневая модель, сочетающая клиент-серверный подход с распределенными технологиями блокчейн и децентрализованного хранения данных лежит в основе архитектуры.

Система состоит из следующих ключевых компонентов:

- Клиентская часть реализована в виде веб-приложения на базе React.js и мобильных приложений для платформ iOS и Android. Клиентское приложение обеспечивает пользовательский интерфейс и выполняет операции по шифрованию и расшифровке данных непосредственно на устройстве пользователя, что является основой для реализации сквозного шифрования.
- Серверная часть построена на основе микросервисной архитектуры, где каждый сервис отвечает за определенный аспект функционирования системы. Взаимодействие между сервисами осуществляется через защищенные каналы с использованием REST API и асинхронного обмена сообщениями.
- Блокчейн-компонент, реализованный на базе Hyperledger Fabric, обеспечивает неизменяемый распределенный реестр для хранения метаданных сообщений и управления криптографическими ключами. Выбор Hyperledger Fabric обусловлен его возможностями по созданию приватных сетей с гибкими политиками доступа и высокой производительностью транзакций.
- Система хранения сообщений представляет собой комбинацию реляционной базы данных PostgreSQL для структурированных данных и распределенной файловой системы IPFS для эффективного хранения зашифрованных сообщений и вложений. Такой подход обеспечивает оптимальное сочетание производительности и отказоустойчивости.
- Криптографический слой, построенный на базе библиотеки Libsodium, предоставляет высокоуровневые примитивы для шифрования, цифровой подписи и хеширования данных. Использование проверенной криптографической библиотеки минимизирует риски, связанные с самостоятельной реализацией криптографических алгоритмов.

Компоненты системы взаимодействуют между собой следующим образом:

- Клиентское приложение устанавливает защищенное соединение с API-шлюзом серверной части, который маршрутизирует запросы к соответствующим микросервисам.
- Микросервисы обрабатывают бизнес-логику, взаимодействуют с базой данных и блокчейн-сетью, а также координируют процессы хранения и извлечения данных из IPFS.
- Блокчейн-сеть Hyperledger Fabric обеспечивает консенсус между узлами и выполнение смарт-контрактов (чейнкодов), реализующих логику работы с метаданными сообщений.
- IPFS обеспечивает распределенное хранение зашифрованных сообщений с возможностью адресации по содержимому, что повышает отказоустойчивость системы.

Схема взаимодействия компонентов представлена на рисунке.

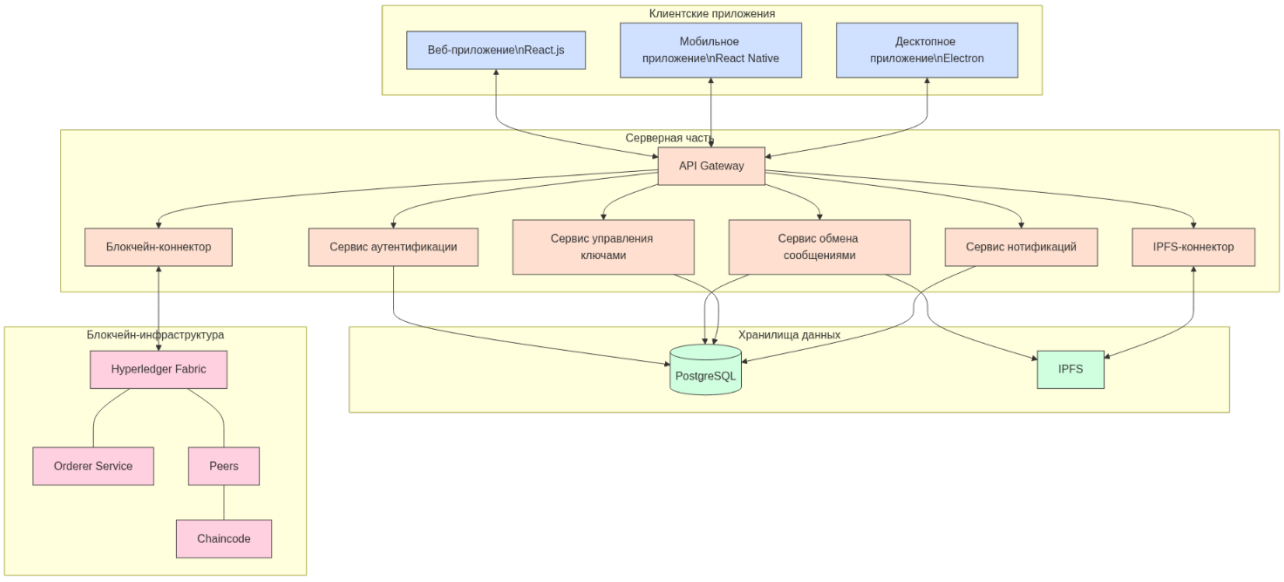

Рис. Схема взаимодействия компонентов СОС

Выводы по работе

Таким образом, в результате проделанной работы был выявлен ряд недостатков в традиционных системах обмена сообщениями. Спроектированная система позволит превзойти их по уровню безопасности без потери производительности за счет гибридной архитектуры, где критически важные метаданные хранятся в блокчейне, а контент – в распределенном хранилище.

Литература

1. Collins R. Blockchain: a new architecture for digital content // EContent. 2016. Vol. 39. № 8. P. 22-23.

2. Hyperledger. Hyperledger Project // Linux Foundation [Электронный ресурс]. 2015. – URL: https://www.hyperledger.org/ (дата обращения 18.01.2021).

3. Libsodium: A modern, portable, easy to use crypto library // [Электронный ресурс]. URL: https://doc.libsodium.org/ (дата обращения: 10.05.2025).

4. Sukhwani H., Martinez M., Chang X., Trivedi S., Rindos A. Performance modeling of PBFT consensus process for permissioned blockchain network // IEEE 36th Symposium on Reliable Distributed Systems (SRDS). 2017. P. 253-255.

5. Равал С. Децентрализованные приложения. Технология Blockchain в действии. СПб.: Питер, 2017. 240 с.

6. Филяк П.Ю., Постников М.К., Федоров С.Е. Применение технологий blockchain для разработки корпоративной информационной системы в защищённом исполнении // Информация и безопасность. 2020. Т. 23. № 3. С. 399-408.

LYGAREV Maksim Sergeevich
Student, MIREA – Russian Technological University,
Russia, Moscow

GULYAEV Aleksandr Yurievich
Candidate of Technical Sciences, Associate Professor,
MIREA – Russian Technological University, Russia, Moscow

DESIGNING THE ARCHITECTURE OF A SECURE MESSAGING SYSTEM USING BLOCKCHAIN TECHNOLOGY

Abstract. *The article presents the architecture of a secure messaging system. A scheme of interaction of the system components was developed. During the comparative analysis, shortcomings in traditional messaging systems were discovered. Based on the results, a conclusion was made about the need to create the designed system. This will increase the level of information transfer security and improve work efficiency.*

Keywords: *information security, information, messaging system, architecture, blockchain.*

СЫРЧИН Александр Владимирович
магистрант, Пермский национальный исследовательский политехнический университет,
Россия, г. Пермь

МЫЛЬНИКОВ Леонид Александрович
кандидат технических наук, доцент,
Пермский национальный исследовательский политехнический университет,
Россия, г. Пермь

ВЫБОР ТЕХНОЛОГИЙ ПРОИЗВОДСТВА ЖГУТОВ ПРОВОДОВ ДЛЯ ОБЕСПЕЧЕНИЯ РАБОТОСПОСОБНОСТИ ЭЛЕКТРОННЫХ КОМПОНЕНТОВ В МАШИНОСТРОЕНИИ

Аннотация. *В статье проведен обзор и сравнение наиболее распространенных технологий производства жгутов проводов (ручное, кооперативное, поточное, модульное и роботизированное производство) по ключевым параметрам эффективности. Проведен обзор задач и параметров, для которых наибольшую эффективность показывают разные технологии, сравнение технологий и принципы выбора технологии производства в зависимости от требований. Показано, что в зависимости от условий функционирования и типов жгутов выбор способ производства может отличаться.*

Ключевые слова: *жгут проводов, производительность, методы выбора, типы жгутов, способы производства жгутов, характеристики жгутов, критерии выбора.*

Введение

Актуальность выбора технологий производства жгутов проводов в современном машиностроении обусловлена стремительным развитием электронных систем, что приводит к значительному увеличению сложности электропроводки во всех отраслях промышленности. Жгуты проводов являются ключевым элементом многокомпонентных и разнесенных электрических систем, обеспечивающим функционирование различных машин и механизмов. Жгуты используются для организации управления бортовыми системами, связи, освещения и обеспечения работы электронных компонентов, служат для создания цепей питания и сигнальных линий.

С момента появления электронной техники наблюдается непрерывное её усложнение и увеличение количества и длины проводов. В последние 20 лет эта тенденция существенно ускорилась в технических системах.

В соответствии с отчетом компании «Boeing» в авиационной промышленности за этот период [8]: средняя длина проводов в пассажирских самолетах выросла с 50 км до 120 км; количество проводов увеличилось с 150 шт. до 500 шт.

Аналогичная ситуация наблюдается и в железнодорожной промышленности [5, с. 54-55]. Изменения стали резко ускоряться при переходе на скоростное железнодорожное сообщение: в высокоскоростных поездах длина электропроводки достигает 80–100 км; за последнее десятилетие количество жгутов увеличилось на 150%, а технологическая сложность систем управления возросла на 250%.

Жгуты проводов широко применяются и в других отраслях промышленности, включая автомобилестроение, медицинское оборудование и энергетику, где они обеспечивают надежное электрическое соединение между компонентами сложных систем.

Низкое качество изготовления жгутов, может приводить к изменению их характеристик и неисправностям, что, в свою очередь может стать причиной отказа техники, дорогостоящего её ремонта, остановки производственных процессов.

Согласно, исследованию «Siemens Mobility. Electrical Systems in Modern Trains», проблемы с электропроводкой составляют до 42% всех технических отказов бортовых систем коммерческих самолетов [9]. Из них по причине неисправных жгутов проводов 45% согласно данным «Wiring System Reliability Study» [1, с. 37-40].

На данный момент большая часть процесса производства жгутов проводов остается ручной, что создает ограничения по производительности и качеству.

Согласно, исследованию «Future of Wire Harness Manufacturing», внедрение автоматизированных решений в производство жгутов проводов может увеличить производительность на 35% [10]. Автоматизация производства жгутов позволяет снизить уровень брака на 30–45%, о чем говорит статья «Global Wire Harness Market Analysis» [11].

Ускорение процесса производства жгутов проводов является критически важным для обеспечения конкурентоспособности предприятий машиностроительной отрасли. Это позволяет: снижать себестоимость продукции; повышать качество выпускаемых изделий; сокращать сроки производства; уменьшать количество брака; оптимизировать производственные процессы.

Однако создание и использование автоматических и автоматизированных линий несет большие затраты на их создание и может удорожать производство единицы продукции при штучном, опытном и мелкосерийном производстве. В связи с этим выбор способа производства является актуальной задачей с учетом высокой стоимости самих проводов (особенно при использовании проводов из дорогостоящих металлов), требований по срокам и надежности.

Сравнение существующих решений

В настоящее время при производстве жгутов проводов находят применение такие технологии как:

- *Ручное производство.* Обеспечивает высокую гибкость за счет полного человеческого контроля, но с ограниченной производительностью.
- *Производство на основе кооперативного принципа (Cellular Manufacturing)*. В отличие от вышесказанных технологий, использует мультифункциональные команды операторов, работающих в специализированных ячейках. Это позволяет быстро перенастраивать процесс под разные типы продукции без необходимости полной автоматизации.
- *Технология поточного производства с использованием передвижных столов (Flow-Line Production with Mobile Workstations).* Организует процесс как непрерывную линию с мобильными рабочими станциями, где каждая станция выполняет конкретные операции, что минимизирует простои и оптимизирует поток материалов, сохраняя при этом человеческий контроль над качеством.
- *Модульное производство (Modular Manufacturing).* Делит процесс изготовления жгута на отдельные блоки или модули. Каждый модуль собирается независимо, а затем все они объединяются в единый жгут. Такой подход упрощает контроль качества и повышает гибкость.
- *Производство с использованием роботизированных рабочих центров (Robotic Workcell Production)*. Роботизированные рабочие центры выполняют повторяющиеся операции, такие как обжимка и маркировка. Финальная сборка остается ручной или полуавтоматической для контроля качества. Технология обеспечивает высокую точность и производительность.

Каждая область машиностроения предъявляет специфические требования к жгутам проводов. Например, если рассмотреть авиационную промышленность и ж/д транспорт, то такую разницу можно увидеть в характеристиках, приведенных в таблице 1.

Таблица 1

Требования, предъявляемые к жгутам проводов в авиационной и ж/д отраслях

Требования	Авиационная промышленность	Железнодорожная промышленность
Температурный режим	От -60°C до +200°C	От -40°C до +40°C
Устойчивость к вибрации	10–20 кГц.	1–5 кГц.
Электромагнитная защита	⩾ 60 дБ (стандарт IEC 61000)	⩾ 40 дБ (для сигнальных систем)
Стандарты безопасности	EN 3475, DO-160	EN 50155, EN 45545

Для унификации процесса производства производители жгутовой продукции разрабатывают унификацию выпускаемой номенклатуры. Выпускаемые типы жгутов соответствует специфическим условиям эксплуатации: например, высокотемпературные жгуты разрабатывались под диапазон температур от -60°C до +200°C и сертификацию DO-160, что

соответствует требованиям авиационной промышленности. Тяговые жгуты разработаны с учетом низкочастотной вибрации до 5 кГц и огнестойкости по EN 45545, что соответствует требованиям ж/д и т. д. (табл. 2).

Таблица 2

Некоторые типы жгутов и их характеристики

Типы жгутов	Высокотемпературные жгуты	Экранированные жгуты	Тяговые жгуты
Отрасль	Авиация	Авиация	Железнодорожный транспорт
Назначение	Работа в условиях высоких температур	Защита от ЭМИ для точной передачи данных	Питание электродвигателей с выдерживанием высоких токов
Длина, м	40–100	10–40	30–70
Кол-во проводников, шт.	20–30	15–20	15–20
Кол-во разъемов, шт.	5–9	3–5	3–8
Сечение проводов, мм^2	2–6	0,5–2	4–8

Для производства всех типов жгутов могут применяться различные технологии производства, которые характеризуются параметрами значения, которых зависят от типа производимой продукции (табл. 3).

Таблица 3

Сравнительная таблица технологий производства в зависимости от изготавливаемых типов жгутов

	Ручное производство	Кооперативное производство	Поточное производство	Модульное производство	Роботизированное производство
Высокотемпературные жгуты					
Время изготовления, мин.	180	120	90	150	30
Стоимость оборудования, тыс. долларов США	0	50	300	100	800
Уровень брака, %	10	6	4	5	1
Операторов на линию	5	3	2	4	1
Сложность. 1–10	2	6	8	5	10
Производительность, жгут/час	1	2	3	2	5
Обслуживание, мес.	–	6	4	5	2
Затраты на обслуживание, тыс. долларов США в год	0	20	50	30	70
Экранированные жгуты					
Время изготовления, мин.	120	90	60	100	20
Стоимость оборудования, тыс. долларов США	0	40	250	80	600
Уровень брака, %	12	7	5	6	2
Операторов на линию	4	3	2	3	1
Сложность. 1–10	3	5	7	4	9
Производительность, жгут/час	1	2	3	2	6

	Ручное производство	Кооперативное производство	Поточное производство	Модульное производство	Роботизированное производство
Обслуживание, мес.	–	6	3	4	2
Затраты на обслуживание, тыс. долларов США в год	0	15	40	25	60
Тяговые жгуты					
Время изготовления, мин.	150	100	45	80	15
Стоимость оборудования, тыс. долларов США	0	60	400	120	900
Уровень брака, %	8	5	3	4	1
Операторов на линию	6	4	2	3	1
Сложность. 1–10	3	7	9	6	10
Производительность, жгут/час	1	2	4	3	8
Обслуживание, мес.	–	5	3	4	1
Затраты на обслуживание, тыс. долларов США в год	0	25	60	35	80

Приведенная в табличном виде формализация позволяет выделить показатели (характеристики для сравнения жгутов) и альтернативы (технологии производства). При этом видно, что эффективность технологий будет связана с объемами производство. Кроме того, не одна из альтернатив не является доминирующей, что делает необходимым использования качественных методов для их выбора [6].

При этом часть факторов связанная с особенностями производственной системы на базе которой планируется организация производства не может быть формализована в явном виде, что делает актуальным применение методов основанных на экспертном выборе (таких, как выбор большинством, метод Делфи, метод Кондорсе, метод с двумя турами, метод Борда, метод отказа от альтернатив, метод анализа иерархий [7], метод анализа сетей и т. п.).

Применение экспертных методов требует выставление оценок для чего может оказаться полезным графическое представление данных. Учитывая разницу в шкалах измерения параметров целесообразным будет проведение нормирования значений показателей:

- для случая, когда лучшими являются наибольшие значения – $X_{норм} = \frac{X - X_{мин}}{X_{макс} - X_{мин}} \times 10$, где X – нормируемый показатель;
- для случая, когда лучшими являются наименьшие значения – $X_{норм} = \frac{X_{макс} - X}{X_{макс} - X_{мин}} \times 10$.

После нормирования на основе данных, приведенных в таблице 3 получим графики (рис.).

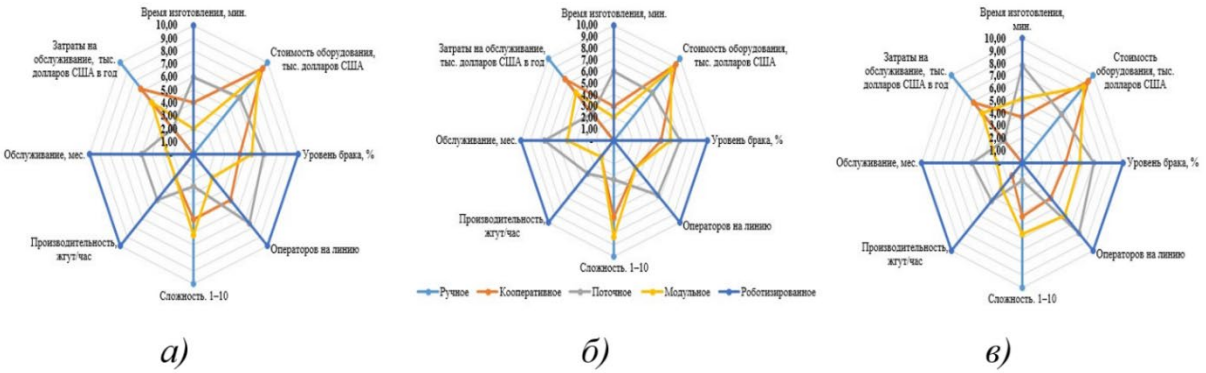

Рис. Визуальное сравнение технологий производства для разных типов жгутов проводов (а) высокотемпературные жгуты, б) экранированные жгуты, в) тяговые жгуты)

Наличие численных оценок не исключает, при наличии целевого/идеального решения и методов, основанных на мерах близости [2, с. 86-93] (среди наиболее известных можно выделить методы оценки отклонений, оценки эффективности, DEA [4, с. 261-278], оценки отклонений со взвешенными суммами, геометрический подход), а также группы методов исключения (TOPSIS, ELECTRE, VIKOR, PROMETHEE).

Таблица 4

Ранжирование технологий и баллы

Типы жгутов	Технологии	Суммарный балл	Ранг
Высокотемпературные (Авиационная промышленность)	Роботизированное	75,00	1
	Поточное	56,55	2
	Кооперативное	44,80	3
	Модульное	41,44	4
	Ручное	25,00	5
Экранированные (Авиационная промышленность)	Роботизированное	75,00	1
	Поточное	56,75	2
	Кооперативное	41,92	4
	Модульное	45,42	3
	Ручное	25,00	5
Тяговые (Железнодорожная промышленность)	Роботизированное	75,00	1
	Поточное	58,14	2
	Кооперативное	40,27	4
	Модульное	51,83	3
	Ручное	25,00	5

На основе ранжирования, выполненного методом ELECTRE [3, с. 1265-1274] можно сделать вывод, что роботизированное производство является безусловным лидером для всех типов жгутов, благодаря максимальным показателям по времени, браку и производительности, однако его внедрение требует значительных капитальных вложений. Поточное производство представляет собой лучший компромисс между стоимостью и эффективностью и рекомендуется для массового серийного выпуска тяговых жгутов, где важны стабильность и умеренные затраты. Модульное производство занимает промежуточную позицию и подходит для малых серий с переменными требованиями, особенно для экранированных жгутов, где оно опережает кооперативное по балансу качества и экономичности. Кооперативное производство остается рентабельным вариантом для ограниченных бюджетов, но уступает по производительности и обслуживанию, в то время как, ручное производство является наименее эффективным и применимо только для уникальных заказов.

Выводы

На основе имеющихся данных можно сделать вывод, что роботизированное производство демонстрирует наивысшую производительность (до 8 для тяговых, 6 для экранированных и 5 для высокотемпературных жгутов проводов) и минимальный уровень брака (1-2%), что обусловлено автоматизацией операций, однако его внедрение связано с высокими капитальными вложениями (до 900 тыс. долларов США), что ограничивает применение в условиях низких объемов производства. Поточное и кооперативное производство обеспечивают компромисс между скоростью (2–4 жгута/час) и экономической эффективностью, особенно для серийных заказов(например, поточная линия для тяговых жгутов с сечением 4–8 мм² обеспечивает 4 жгута/час при 3% брака и общей стоимостью оборудования 400 тыс. долларов США, тогда как кооперативные ячейки для авиационных высокотемпературных жгутов (длина 40–100 м) гарантируют 2 жгута/час при 6% брака). Ручное производство, несмотря на нулевые начальные вложения, характеризуется низкой скоростью (1 жгут/час) и высоким уровнем брака (до 12%), что делает его непригодным при промышленном производстве, за исключением случаев уникальных заказов, требующих индивидуальной настройки под стандарты EN 3475 или EN 45545.

Подобные рассуждения помогают эксперту сделать вывод и, тем самым, формализовать свое мнение для применения с использованием методов коллективного выбора.

На качественном уровне обзор технологий производства жгутов проводов выявил их

специфическую применимость в зависимости от масштаба и требований производства. Ручная и модульная технологии производства остаются оптимальными для мелкосерийных заказов. Роботизированное производство, демонстрируя оптимальные показатели по времени, браку и производительности, становится технологией выбора для крупносерийного производства жгутов в авиационной и железнодорожной промышленностях.

Литература

1. Krasnov D., Stepanov E. Application of the nx and e3 series programs for electrical routing of wiring and harness Bryansk State Technical University, 2019. P. 37-40.

2. Kuetz M. IT-Prozesse mit Kennzahlen steuern // Controlling & Management Review. 2014. № 7 (58). P. 86-93.

3. Reginaldo F. Portfolio Management in Brazil and a Proposal for Evaluation and Balancing of Portfolio Projects with ELECTRE TRI and IRIS // Procedia Computer Science. 2015. (55). P. 1265-1274.

4. Sharifghazvini M. Integration of a new MCDM approach based on the DEA, FANP with MONLP for efficiency-risk assessment to optimize project portfolio by branch and bound: a real case study // Economic computation and economic cybernetics studies and research. 2018. № 1 (52). P. 261-278.

5. Горбач А. Диверсификация трансфера технологий и современного оборудования для опытного и мелкосерийного жгутового производства ОПК России // Технологии в электронной промышленности. 2017. № 6. С. 54-55.

6. Мыльников Л.А. Управление проектами и системами в условиях цифровой экономики / Л.А. Мыльников, Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2021. 130 с.

7. Саати Т. Принятие решений. Метод анализа иерархий. / Т. Саати, Москва: Радио и связь, 1993. 278 с.

8. Boeing. Commercial Airplane Weight Growth Trends [Электронный ресурс]. URL: https://www.boeing.com/commercial/aeromagazine/articles/qtr_4_07/article_04_1.html.

9. Siemens Mobility. Electrical Systems in Modern Trains [Электронный ресурс]. URL: https://www.siemens.com/mobility/global/en/products/rail-vehicles/innovations/electrical-systems.html.

10. Deloitte. Future of Wire Harness Manufacturing [Электронный ресурс]. URL: https://www2.deloitte.com/us/en/insights/focus/future-of-manufacturing/wire-harness-manufacturing.html.

11. Frost & Sullivan. Global Wire Harness Market Analysis [Электронный ресурс]. URL: https://www.frost.com/report/global-wire-harness-market-analysis.

SYRCHIN Alexander Vladimirovich
Master's Student, Perm National Research Polytechnic University, Russia, Perm

MYLNIKOV Leonid Aleksandrovich
Candidate of Technical Sciences, Associate Professor,
Perm National Research Polytechnic University, Russia, Perm

THE CHOICE OF TECHNOLOGIES FOR THE PRODUCTION OF WIRING HARNESSES TO ENSURE THE OPERABILITY OF ELECTRONIC COMPONENTS IN MECHANICAL ENGINEERING

Abstract. *The article provides an overview and comparison of the most common technologies for the production of wiring harnesses (manual, cooperative, in-line, modular and robotic production) according to key performance parameters. An overview of the tasks and parameters for which* different *technologies show the greatest efficiency, a comparison of technologies and the principles of choosing a production technology depending on the requirements is carried out. It is shown that depending on the operating conditions and types of harnesses, the choice of the production method may vary.*

Keywords: *wiring harness, performance, selection methods, types of harnesses, production methods of harnesses, characteristics of harnesses, selection criteria.*

ФРЕНКИН Эмиль Константинович
магистрант,
Азербайджанский государственный университет нефти и промышленности,
Азербайджан, г. Баку

АРХИТЕКТУРА ОБЛАЧНЫХ ВЕБ-ПРИЛОЖЕНИЙ ДЛЯ УПРАВЛЕНИЯ СТРОИТЕЛЬНЫМИ ПРОЦЕССАМИ: ОПЫТ РАЗРАБОТКИ WAREHOUSEHUB

Аннотация. *В статье представлен подход к разработке облачного веб-приложения WarehouseHub для управления строительными процессами, включая объекты аграрной инфраструктуры, такие как склады и логистические центры. Описана архитектура, основанная на технологиях React, Node.js и Express, обеспечивающая масштабируемость, производительность и удобство интеграции. Рассмотрены функциональные возможности: авторизация пользователей, управление ролями и ведение истории действий с использованием localStorage. Показана актуальность облачных технологий для цифровизации строительной отрасли и их потенциал для аграрного сектора. Проведено сравнение с аналогичными системами, демонстрирующее преимущества WarehouseHub. Статья адресована специалистам в области информационных технологий, строительства и аграрного управления.*

Ключевые слова: *облачные технологии, веб-приложения, строительство, аграрная инфраструктура, управление, React, Node.js, Express, архитектура, авторизация, localStorage.*

Введение

Цифровизация строительной отрасли, включая управление объектами аграрной инфраструктуры, такими как склады для сельскохозяйственной продукции, требует внедрения современных информационных систем. Облачные веб-приложения обеспечивают доступность данных, автоматизацию процессов и эффективную координацию участников проектов [1]. В условиях роста аграрного сектора, где строительство логистических центров и складов играет ключевую роль, специализированные системы управления становятся критически важными.

Разработанное веб-приложение WarehouseHub решает задачи управления строительными процессами, включая учет ресурсов, контроль действий и обеспечение взаимодействия между участниками. Цель исследования – разработка и описание архитектуры WarehouseHub, демонстрация ее функциональных возможностей и оценка применимости в строительной и аграрной отраслях. Задачи включают:

- Анализ требований к облачным системам.
- Проектирование архитектуры на основе React, Node.js и Express.
- Реализацию функционала авторизации и управления данными.
- Сравнение с аналогичными решениями.

В статье использованы методы системного анализа, проектирования программного обеспечения, тестирования и сравнительного анализа.

Материалы и методы

WarehouseHub разработан с использованием стека технологий, обеспечивающего высокую производительность и гибкость:

- **React**: библиотека для создания интерактивного интерфейса с компонентным подходом, оптимизированная для быстрого рендеринга.
- **Node.js и Express**: серверная платформа и фреймворк для построения REST API, обеспечивающего взаимодействие между клиентом и сервером.
- **localStorage**: механизм хранения данных на стороне клиента для кэширования истории действий и пользовательских настроек.

Методология разработки включала следующие этапы:

1. **Сбор требований**: Определены ключевые функции, включая управление складскими запасами, авторизацию, разграничение ролей

(администратор, менеджер, сотрудник) и логирование действий.

2. **Проектирование архитектуры**: Разработана клиент-серверная модель с REST API, где клиентская часть отвечает за интерфейс, а серверная – за обработку данных и безопасность.

3. **Реализация**: Создан фронтенд на React и бэкенд на Express, интегрированы механизмы авторизации и логирования.

4. **Тестирование**: Проверены функциональность, производительность (время отклика <200 мс) и устойчивость к нагрузкам.

Архитектура WarehouseHub представлена следующим образом:

- **Клиентская часть**: React-компоненты для панели управления, списков ресурсов и форм.
- **Серверная часть**: Express-сервер с REST API для обработки запросов.
- **Хранилище данных**: localStorage для временных данных, синхронизируемых с сервером.

Для реализации авторизации использован механизм сессий (Express-session), а для логирования действий – комбинация localStorage и серверной базы данных.

Результаты и обсуждение

Основным результатом исследования является разработка облачного веб-приложения WarehouseHub, включающего следующие компоненты и функциональные возможности:

1. Клиентская часть:

Интерфейс включает панель управления, списки складских запасов, формы ввода данных и историю действий.

Производительность оптимизирована за счет виртуального DOM и минимизации запросов к серверу.

Пример компонента React для отображения истории действий:

```
function ActionHistory() {
 const [history, setHistory] = useState(JSON.parse(localStorage.getItem('actions')) || []);
 useEffect(() => {
 const updateHistory = () => {
setHistory(JSON.parse(localStorage.getItem('actions')) || []);
 };
 window.addEventListener('storage', updateHistory);
 return () => window.removeEventListener('storage', updateHistory);
 }, []);
 return (
 <div>
 <h2>История действий</h2>
 <ul>
 {history.map((action, index) => (
 <li key={index}>{action.user}: {action.action} ({action.time})</li>
 ))}
 </ul>
 </div>
 );
}
```

2. Серверная часть:

REST API на Express обеспечивает маршруты для авторизации, управления ролями и логирования.

Пример маршрута для логирования действий:

```
app.post('/api/log', (req, res) => {
 const { user, action, time } = req.body;
 // Сохранение в базе данных (здесь упрощено)
 console.log(`Log: ${user} performed ${action} at ${time}`);
 res.status(200).json({ message: 'Action logged' });
});
```

3. Локальное хранилище:

localStorage используется для кэширования истории действий, что снижает нагрузку на сервер и ускоряет доступ к данным.

Данные синхронизируются с сервером при подключении к сети.

Пример функции логирования:

```
function logAction(user, action) {
 const history = JSON.parse(localStorage.getItem('actions')) || [];
 const newAction = { user, action, time: new Date().toISOString() };
 history.push(newAction);
 localStorage.setItem('actions', JSON.stringify(history));
 // Отправка на сервер
 fetch('/api/log', {
 method: 'POST',
 headers: { 'Content-Type': 'application/json' },
```

```
  body: JSON.stringify(newAction)
  });
}
```

4. Применимость в аграрной отрасли:

WarehouseHub адаптирован для управления строительством аграрных объектов, таких как склады для зерна или логистические центры. Система позволяет:

- Учитывать строительные материалы (цемент, металл) и их расход.
- Координировать работу подрядчиков и сотрудников.
- Отслеживать действия для обеспечения прозрачности.

Пример сценария: менеджер склада использует WarehouseHub для проверки поступления материалов, а администратор контролирует действия через историю.

Сравнение с аналогами

WarehouseHub сравнивался с традиционными системами управления, такими как Microsoft Excel и локальные ERP-системы (например, 1С):

Преимущества WarehouseHub:

- Облачный доступ, не требующий установки ПО.
- Гибкость интеграции с другими системами через REST API.
- Удобный интерфейс на React, адаптированный для мобильных устройств.

Недостатки:

- Зависимость от интернет-соединения.
- Ограниченные возможности localStorage (размер до 5 МБ, уязвимость к атакам на стороне клиента).

По сравнению с зарубежными аналогами, такими как Procore или PlanGrid, WarehouseHub проще в развертывании и дешевле, что важно для малых и средних предприятий в аграрной отрасли. Однако зарубежные системы предлагают более развитую аналитику, что является направлением для дальнейшего развития.

Ограничения и перспективы

Основное ограничение – зависимость от интернет-соединения, что может затруднять использование в удаленных аграрных регионах. Для решения этой проблемы планируется внедрение оффлайн-режима с локальной базой данных (IndexedDB). Также рассматривается интеграция модулей машинного обучения для прогнозирования расхода материалов.

Заключение

Разработанное приложение WarehouseHub демонстрирует эффективность облачных технологий для управления строительными процессами, включая аграрные объекты. Архитектура, основанная на React, Node.js и Express, обеспечивает производительность, масштабируемость и удобство использования. Функционал авторизации, управления ролями и логирования действий отвечает требованиям строительной и аграрной отраслей. В дальнейшем планируется расширение функционала, включая оффлайн-режим и аналитические модули, что повысит применимость системы в условиях цифровизации.

Литература

1. Мижериков В.А. Информационные технологии в управлении. – М.: Информатика, 2005.
2. Fowler M. Patterns of Enterprise Application Architecture. – Addison-Wesley, 2002.
3. Коваленко А.П. Цифровизация строительной отрасли: тенденции и вызовы // Вестник РИНЦ, 2023. – № 4. – С. 45-50.
4. React Documentation. – URL: https://reactjs.org/docs (дата обращения: 19.05.2025).
5. Express Documentation. – URL: https://expressjs.com (дата обращения: 19.05.2025).
6. Иванов С.В. Облачные технологии в управлении проек compassion:// Информационные системы, 2024. – № 2. – С. 33-39.
7. ГОСТ 7.1-2003. Библиографическая запись. Общие требования и правила составления.

FRENKIN Emil Konstantinovich
Master's Student, Azerbaijan State University of Petroleum and Industry,
Azerbaijan, Baku

ARCHITECTURE OF CLOUD-BASED WEB APPLICATIONS FOR CONSTRUCTION PROCESS MANAGEMENT: THE DEVELOPMENT EXPERIENCE OF WAREHOUSEHUB

Abstract. *The article presents an approach to developing a cloud-based web application called WarehouseHub for managing construction processes, including agricultural infrastructure facilities such as warehouses and logistics centers. The architecture based on React and Node technologies is described.js and Express, providing scalability, performance, and ease of integration. The functionality is considered: user authorization, role management, and action history management using localStorage. The relevance of cloud technologies for the digitalization of the construction industry and their potential for the agricultural sector is shown. A comparison with similar systems has been carried out, demonstrating the advantages of the WarehouseHub. The article is addressed to specialists in the field of information technology, construction and agricultural management.*

Keywords: *cloud technologies, web applications, construction, agricultural infrastructure, management, React, Node.js, Express, architecture, authorization, localStorage.*

ФРЕНКИН Эмиль Константинович
магистрант,
Азербайджанский государственный университет нефти и промышленности,
Азербайджан, г. Баку

БЕЗОПАСНОСТЬ И УПРАВЛЕНИЕ ДАННЫМИ В ОБЛАЧНЫХ ВЕБ-ПРИЛОЖЕНИЯХ СТРОИТЕЛЬНОЙ ОТРАСЛИ: ПОДХОДЫ НА ОСНОВЕ WAREHOUSEHUB

Аннотация. *В статье рассматриваются подходы к обеспечению безопасности и управлению данными в облачном веб-приложении WarehouseHub, разработанном для управления строительными процессами, включая аграрную инфраструктуру, такую как склады и логистические центры. Описаны механизмы авторизации, управления ролями пользователей и ведения истории действий с использованием технологий React, Node.js, Express и localStorage. Рассмотрены методы защиты данных, минимизации уязвимостей и обеспечения целостности информации. Показана применимость решения в аграрной отрасли, где безопасность данных критически важна. Результаты демонстрируют устойчивость системы к основным угрозам и ее эффективность для строительных проектов. Статья адресована специалистам в области информационных технологий, строительства и аграрного управления.*

Ключевые слова: *облачные технологии, веб-приложения, строительство, аграрная инфраструктура, безопасность, авторизация, управление данными, React, Node.js, Express, localStorage.*

Введение

Облачные веб-приложения, применяемые в строительной отрасли, обрабатывают конфиденциальные данные, такие как планы проектов, складские запасы, финансовая информация и логистические цепочки. В аграрной инфраструктуре, включающей строительство складов для сельскохозяйственной продукции, безопасность и эффективное управление данными становятся ключевыми задачами [1, с. 12-18]. Утечка данных или несанкционированный доступ могут привести к значительным финансовым и репутационным потерям, что особенно критично в условиях цифровизации аграрного сектора.

Цель исследования – разработка и описание подходов к обеспечению безопасности и управлению данными в облачном веб-приложении WarehouseHub. Задачи включают:

- Анализ потенциальных угроз и уязвимостей.
- Реализацию механизмов авторизации и разграничения доступа.
- Оценку эффективности предложенных решений в контексте строительной и аграрной отраслей.
- Сравнение с аналогичными системами управления.

В статье использованы методы анализа безопасности, проектирования программного обеспечения, тестирования и сравнительного анализа.

Материалы и методы

WarehouseHub разработан с использованием современного стека технологий, обеспечивающего безопасность и производительность:

- **React**: библиотека для создания отзывчивого и безопасного пользовательского интерфейса с компонентным подходом.
- **Node.js и Express**: серверная платформа и фреймворк для реализации REST API, поддерживающего функции авторизации, управления данными и логирования.
- **localStorage**: механизм хранения данных на стороне клиента для кэширования временных данных, таких как история действий и пользовательские настройки.

Методология разработки включала следующие этапы:

1. **Анализ угроз**: Идентифицированы основные риски, включая XSS (межсайтовый скриптинг), CSRF (подделка межсайтовых запросов), утечку данных через localStorage и несанкционированный доступ.
2. **Проектирование безопасности**: Разработаны механизмы авторизации на основе

сессий, разграничения доступа по ролям и защиты данных.

3. **Реализация**: Внедрены функции авторизации (Express-session), управления ролями и логирования действий с синхронизацией между localStorage и сервером.

4. **Тестирование**: Проведены тесты на устойчивость к атакам, производительность (время отклика <200 мс) и целостность данных.

Безопасность WarehouseHub обеспечивается следующими мерами:

- **Авторизация**: Используется сессионная авторизация с Express-session для проверки подлинности пользователей.
- **Роли пользователей**: Реализованы три уровня доступа: администратор (полный доступ), менеджер (управление ресурсами), сотрудник (ограниченный доступ).
- **Логирование**: Действия пользователей сохраняются в localStorage и синхронизируются с серверной базой данных для обеспечения прозрачности.
- **Защита данных**: Применены заголовки HTTP (например, X-Content-Type-Options, X-Frame-Options) для предотвращения атак.

Результаты и обсуждение

Разработка WarehouseHub позволила реализовать комплекс механизмов безопасности и управления данными, обеспечивающих надежность и эффективность системы. Основные результаты включают:

1. Механизм авторизации:

Использована сессионная авторизация с Express-session, обеспечивающая безопасное управление пользовательскими сеансами.

Пример кода для настройки сессий и авторизации:

```
const session = require('express-session');
app.use(session({
 secret: 'warehousehub_secret_key',
 resave: false,
 saveUninitialized: false,
 cookie: { secure: false } // В продакшене использовать secure: true
}));
app.post('/login', (req, res) => {
 const { username, password } = req.body;
 // Упрощенная проверка учетных данных
 if (username === 'admin' && password === 'password') {
 req.session.user = username;
 req.session.role = 'admin';
 res.json({ message: 'Logged in successfully' });
 } else {
 res.status(401).json({ message: 'Invalid credentials' });
 }
});
```

2. Управление ролями пользователей:

Реализованы роли: администратор (управление пользователями и данными), менеджер (контроль ресурсов), сотрудник (доступ только к своим задачам).

Пример middleware для ограничения доступа по ролям:

```
function restrictTo(role) {
 return (req, res, next) => {
 if (req.session.user && req.session.role === role) {
 next();
 } else {
 res.status(403).json({ message: 'Access denied: insufficient permissions' });
 }
 };
}
app.get('/admin/resources', restrictTo('admin'), (req, res) => {
 res.json({ resources: ['cement', 'steel'] });
});
```

3. Управление данными и логирование:

LocalStorage используется для временного хранения истории действий, что снижает нагрузку на сервер и ускоряет доступ к данным.

Данные синхронизируются с сервером для обеспечения целостности.

Пример функции логирования действий:

```
function logAction(user, action) {
 const history = JSON.parse(localStorage.getItem('actions')) || [];
 const newAction = { user, action, time: new Date().toISOString() };
 history.push(newAction);
 localStorage.setItem('actions', JSON.stringify(history));
 // Асинхронная отправка на сервер
 fetch('/api/log', {
 method: 'POST',
 headers: { 'Content-Type': 'application/json' },
 body: JSON.stringify(newAction)
 }).catch(err => console.error('Log sync failed:', err));
}
```

4. Анализ уязвимостей localStorage:

Основная уязвимость localStorage – доступность данных для XSS-атак, если злоумышленник внедрит вредоносный скрипт.

Для минимизации рисков применены:

- Валидация и санитизация входных данных на стороне сервера.
- Использование заголовков Content-Security-Policy (CSP) для ограничения источников скриптов.
- Ограничение объема данных в localStorage (до 100 записей действий).

Пример настройки CSP:

```
app.use((req, res, next) => {
 res.setHeader("Content-Security-Policy",
"script-src 'self'");
 next();
});
```

Применимость в аграрной отрасли

WarehouseHub адаптирован для управления строительными процессами в аграрной инфраструктуре, например, при строительстве складов для зерна, силосов или логистических центров. Система обеспечивает:

- **Безопасность данных**: Конфиденциальная информация о запасах (например, строительные материалы) защищена от несанкционированного доступа.
- **Прозрачность**: История действий позволяет отслеживать, кто и когда внес изменения в данные о ресурсах.
- **Эффективность**: Менеджеры могут быстро проверять статус поставок, а администраторы – контролировать доступ.

Пример сценария: менеджер склада использует WarehouseHub для регистрации поступления цемента, система фиксирует действие в localStorage и синхронизирует с сервером. Администратор проверяет лог, чтобы убедиться в корректности операции. Это особенно важно в аграрной отрасли, где точный учет материалов влияет на сроки строительства и эксплуатацию объектов.

Сравнение с аналогами

WarehouseHub сравнивался с традиционными системами управления, такими как Microsoft Excel, локальные ERP (например, 1С) и зарубежные облачные платформы (Procore, PlanGrid):

Преимущества WarehouseHub:

- Облачный доступ, не требующий установки сложного ПО.
- Простота интеграции через REST API.
- Адаптация для аграрной инфраструктуры (например, учет материалов для складов).
- Низкая стоимость развертывания по сравнению с Procore.

Домашняя часть:

- Уязвимость localStorage к XSS, требующая дополнительных мер защиты.
- Отсутствие встроенной аналитики, как в Procore или PlanGrid.
- Зависимость от интернет-соединения, что может быть проблемой в удаленных аграрных регионах.

По сравнению с 1С, WarehouseHub предлагает более удобный интерфейс и мобильную адаптацию, что упрощает использование на строительных площадках. Однако 1С превосходит по возможностям бухгалтерского учета, что не является основной целью WarehouseHub.

Ограничения и перспективы

Основное ограничение – уязвимость localStorage к XSS-атакам, что требует внедрения шифрования данных на стороне клиента. Также зависимость от интернет-соединения ограничивает использование в регионах с нестабильной связью. Для решения этих проблем планируется:

- Внедрение шифрования данных в localStorage с использованием библиотеки CryptoJS.
- Разработка оффлайн-режима с локальной базой данных (IndexedDB).
- Интеграция биометрической авторизации для повышения безопасности.

Заключение

Облачное веб-приложение WarehouseHub демонстрирует эффективные подходы к обеспечению безопасности и управлению данными в строительной и аграрной отраслях. Механизмы авторизации, управления ролями и логирования действий, реализованные с использованием React, Node.js, Express и localStorage, обеспечивают конфиденциальность и целостность данных. Система устойчива к основным угрозам, включая XSS и CSRF, и адаптирована для управления строительством аграрных объектов. В дальнейшем планируется усиление защиты данных и расширение функционала, что повысит применимость решения в условиях цифровизации.

Литература

1. Коваленко А.П. Безопасность информационных систем // Информационные технологии, 2023. – №3. – С. 12-18.

2. OWASP Top Ten. – URL: https://owasp.org/www-project-top-ten (дата обращения: 19.05.2025).

3. Express Documentation. – URL: https://expressjs.com (дата обращения: 19.05.2025).

4. Мижериков В.А. Информационные технологии в управлении. – М.: Информатика, 2005.

5. Иванов С.В. Облачные технологии в управлении проектами // Информационные системы, 2024. – №2. – С. 33-39.

6. ГОСТ 7.1-2003. Библиографическая запись. Общие требования и правила составления.

FRENKIN Emil Konstantinovich
Graduate Student, Azerbaijan State University of Petroleum and Industry,
Azerbaijan, Baku

SECURITY AND DATA MANAGEMENT IN CLOUD-BASED WEB APPLICATIONS IN THE CONSTRUCTION INDUSTRY: WAREHOUSE-BASED APPROACHES

Abstract. *The article discusses approaches to security and data management in the cloud-based web application WarehouseHub, designed to manage construction processes, including agricultural infrastructure such as warehouses and logistics centers. Authorization mechanisms, user role management, and action history management using React and Node technologies are described.js, Express, and localStorage. Methods of data protection, minimizing vulnerabilities and ensuring information integrity are considered. The applicability of the solution in the agricultural sector, where data security is critically important, is shown. The results demonstrate the system's resilience to major threats and its effectiveness for construction projects. The article is addressed to specialists in the field of information technology, construction and agricultural management.*

Keywords: *cloud technologies, web applications, construction, agricultural infrastructure, security, authorization, data management, React, Node.js, Express, localStorage.*

АРХИТЕКТУРА, СТРОИТЕЛЬСТВО

ПЕРМЯКОВА Надежда Анатольевна
студентка, Ижевский государственный технический университет имени М. Т. Калашникова, Россия, г. Ижевск

Научный руководитель – доцент кафедры промышленного и гражданского строительства Ижевского государственного технического университета имени М. Т. Калашникова, кандидат педагогических наук Кислякова Юлия Геннадьевна

ПРОБЛЕМЫ ХРАНЕНИЯ И УЧЕТА ПРОЕКТНО-СМЕТНОЙ ДОКУМЕНТАЦИИ В СТРОИТЕЛЬНЫХ ОРГАНИЗАЦИЯХ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ИХ РЕШЕНИЯ

Аннотация. *В статье рассматриваются актуальные проблемы хранения и учета проектно-сметной документации в строительных организациях в условиях цифровизации отрасли. Проведен комплексный анализ существующих организационных, технических и экономических проблем в данной области. Предложены современные подходы к их решению, основанные на внедрении цифровых технологий, включая BIM-моделирование, системы электронного документооборота, облачные технологии и искусственный интеллект. Разработана концепция многоуровневой системы управления проектно-сметной документацией, учитывающая специфику строительной отрасли. Представлены практические рекомендации по внедрению предложенных решений и оценке их экономической эффективности. Результаты исследования имеют практическую значимость для строительных организаций различного масштаба, стремящихся оптимизировать процессы управления документацией.*

Ключевые слова: *проектно-сметная документация, строительная организация, электронный документооборот, BIM-технологии, информационная безопасность, цифровизация строительства, управление документацией, облачные технологии, искусственный интеллект, система архивирования.*

Введение

В современных условиях интенсивного развития строительной отрасли особую актуальность приобретают вопросы эффективной организации хранения и учета проектно-сметной документации. Строительные организации ежедневно сталкиваются с необходимостью обработки, систематизации и хранения значительных объемов технической документации, что требует внедрения современных подходов к организации документооборота.

Актуальность исследования обусловлена рядом факторов. Во-первых, увеличением объемов строительства в Российской Федерации (по данным Росстата, в 2023 году объем строительных работ вырос на 7,8% по сравнению с предыдущим годом), что влечет за собой пропорциональный рост объемов проектно-сметной документации. Во-вторых, ужесточением требований к хранению и учету документации со стороны контролирующих органов. В-третьих, необходимостью оптимизации затрат на хранение и обработку документации при одновременном повышении эффективности доступа к ней.

Несмотря на активное внедрение цифровых технологий в строительную отрасль, проблема организации эффективного хранения и учета проектно-сметной документации остается недостаточно изученной. Существующие исследования в данной области носят фрагментарный характер и не предлагают комплексного решения выявленных проблем.

Целью исследования является разработка научно обоснованных рекомендаций по совершенствованию системы хранения и учета проектно-сметной документации в строительных организациях.

Для достижения поставленной цели определены следующие задачи:

- провести анализ существующих подходов к организации хранения и учета проектно-сметной документации;
- выявить и систематизировать основные проблемы в данной области;
- исследовать современные технологические решения для организации документооборота.

Методологическую основу исследования составляют общенаучные методы познания, включая анализ, синтез, сравнение и обобщение, а также специальные методы: статистический анализ, экспертные оценки, системный подход к изучению организационно-технических проблем.

Научная новизна исследования заключается в разработке комплексного подхода к решению проблем хранения и учета проектно-сметной документации, учитывающего современные технологические возможности и специфику строительной отрасли. В работе предложена оригинальная методика оценки эффективности систем хранения документации, а также разработан алгоритм внедрения современных технологических решений в существующую систему документооборота строительных организаций.

Практическая значимость работы определяется возможностью использования полученных результатов для совершенствования систем документооборота в строительных организациях различного масштаба, что позволит повысить эффективность их деятельности и снизить операционные издержки.

Анализ существующих проблем хранения и учета проектно-сметной документации

Проведенное исследование позволило выявить ряд существенных проблем в области хранения и учета проектно-сметной документации в строительных организациях. В организационном аспекте наиболее острой является проблема отсутствия единой системы классификации и кодификации документов. Существенные трудности создает нечеткое распределение ответственности между подразделениями, а также несовершенство процедур внесения изменений в документацию [5, с. 125-132].

Технический аспект проблемы характеризуется недостаточностью серверных мощностей для хранения постоянно растущих объемов электронной документации. Существенную сложность представляет устаревание форматов хранения данных и несовместимость различных программных продуктов, используемых в процессе проектирования. Процесс перевода документации из бумажного в электронный формат также сопряжен с множеством технических трудностей, усугубляемых отсутствием единых стандартов обмена данными между различными информационными системами [1, с. 128-135].

В современных условиях особую актуальность приобретают вопросы информационной безопасности. Строительные организации сталкиваются с существенными рисками несанкционированного доступа к конфиденциальной информации. Отсутствие надежных систем резервного копирования и уязвимость систем электронного документооборота к кибератакам создают дополнительные риски. Организация разграничения прав доступа и обеспечение целостности электронных документов также представляют серьезную проблему.

Экономическая составляющая вопроса характеризуется значительными затратами на внедрение современных систем электронного документооборота и необходимостью постоянного обучения персонала. Финансовые потери от неэффективной организации хранения и учета документации составляют существенную долю от стоимости проекта, что для крупных строительных объектов выражается в значительных суммах. Эти потери обусловлены временными затратами на поиск необходимых документов, исправление ошибок при работе с устаревшими версиями документации, а также необходимостью повторного создания утерянных документов.

Основные направления решения выявленных проблем

Современное развитие информационных технологий открывает широкие возможности для совершенствования систем хранения и учета проектно-сметной документации. Первостепенное значение приобретает внедрение технологий информационного моделирования зданий (BIM), позволяющих создать единую информационную среду для всех участников строительного процесса. Интеграция BIM-технологий с системами электронного документооборота обеспечивает качественно новый уровень работы с проектной документацией [3, с. 4143].

Совершенствование системы электронного документооборота должно происходить в направлении создания единой цифровой платформы, обеспечивающей полный жизненный цикл проектно-сметной документации. Важным аспектом является внедрение технологий искусственного интеллекта для автоматизации процессов классификации и поиска документов. Использование машинного обучения позволяет существенно повысить точность и скорость обработки документации.

Оптимизация процессов архивирования и поиска документации требует внедрения современных систем индексации и каталогизации. Перспективным направлением является использование технологий распределенных реестров (blockchain) для обеспечения неизменности и прослеживаемости истории изменений документов. Данный подход позволяет создать надежную систему контроля версий документации и обеспечить прозрачность всех производимых изменений.

Развитие облачных технологий хранения данных открывает новые возможности для организации распределенного доступа к проектно-сметной документации. Использование облачных решений позволяет оптимизировать затраты на IT-инфраструктуру и обеспечить высокий уровень доступности документации [4, с. 42-49].

В качестве комплексного решения выявленных проблем предлагается создание многоуровневой системы управления проектно-сметной документацией, включающей следующие основные компоненты. Базовый уровень обеспечивает надежное хранение документации с использованием современных технологий резервного копирования и восстановления данных. Функциональный уровень предоставляет инструменты для работы с документацией, включая средства поиска, классификации и управления версиями. Интеграционный уровень обеспечивает взаимодействие с различными информационными системами и внешними участниками строительного процесса [2, с. 10-15].

Предлагаемые решения должны внедряться поэтапно, с учетом специфики конкретной строительной организации и ее технических возможностей. Важным аспектом является обучение персонала работе с новыми технологиями и формирование культуры электронного документооборота. Экономическая эффективность предложенных мероприятий подтверждается расчетами, показывающими существенное снижение операционных затрат и повышение производительности труда сотрудников.

Заключение

Проведенное исследование позволяет сделать вывод о критической важности эффективной организации хранения и учета проектно-сметной документации для современных строительных организаций. В ходе работы были выявлены и систематизированы основные проблемы в данной области, предложены пути их решения с использованием современных информационных технологий.

Основные результаты исследования свидетельствуют о необходимости комплексного подхода к модернизации систем документооборота, включающего как технологические, так и организационные аспекты. Внедрение предложенных решений позволяет достичь существенного повышения эффективности работы с проектно-сметной документацией, что подтверждается проведенными экономическими расчетами.

Перспективы дальнейших исследований связаны с развитием технологий искусственного интеллекта и их применением в сфере управления строительной документацией. Особый интерес представляет изучение возможностей интеграции систем документооборота с технологиями информационного моделирования зданий и создания единой цифровой среды управления строительными проектами.

Практическая значимость полученных результатов заключается в возможности их непосредственного применения строительными организациями для совершенствования существующих систем хранения и учета документации. Разработанные рекомендации могут быть адаптированы под специфику конкретных организаций и использованы при планировании мероприятий по цифровой трансформации.

В условиях цифровизации строительной отрасли эффективное управление проектно-сметной документацией становится одним из ключевых факторов конкурентоспособности строительных организаций. Реализация предложенных в исследовании решений позволит не только оптимизировать текущие процессы, но и создать надежную основу для дальнейшего развития и внедрения инновационных технологий в строительной сфере.

Результаты исследования могут быть использованы как крупными строительными компаниями, так и небольшими организациями, стремящимися повысить эффективность своей деятельности за счет совершенствования процессов управления документацией. Представленные рекомендации также могут быть полезны при разработке отраслевых стандартов и методических материалов по организации документооборота в строительной отрасли.

Литература

1. Белоусов К.М., Современные подходы к организации электронного документооборота в строительстве // Строительство и архитектура. 2023. № 2. С. 128-135.

2. Галкина О., Кораго Н., Рындин А., Тучков А. Система электронного архива Д'АР – первый шаг к построению системы управления проектными данными // САПР и графика, 2021, № 9. – С. 10-15.

3. Рындин А. Ввод сканированных документов в электронный архив предприятия // CADmaster. 2003. № 1. С. 4143.

4. Тучков А. Внедрение электронных архивов инженерной документации. Попытка обобщения // CADmaster, 2018, № 3. – С. 42-49.

5. Building Information Modeling: Digital Revolution in Construction Industry // Construction Management Journal. 2024. Vol. 15. No. 2. P. 125-132.

PERMYAKOVA Nadezhda Anatolyevna
Student, Izhevsk State Technical University named after M. T. Kalashnikov,
Russia, Izhevsk

Scientific Advisor – Associate Professor of the Department of Industrial and Civil Engineering of Izhevsk State Technical University named after M. T. Kalashnikov, Candidate of Pedagogical Sciences Kislyakova Julia Gennadievna

PROBLEMS OF STORAGE AND ACCOUNTING OF DESIGN ESTIMATES IN CONSTRUCTION ORGANIZATIONS AND THE MAIN DIRECTIONS OF THEIR SOLUTION

Abstract. *The article discusses the current problems of storage and accounting of design estimates in construction organizations in the context of digitalization of the industry. A comprehensive analysis of the existing organizational, technical and economic problems in this area has been carried out. Modern approaches to their solution based on the introduction of digital technologies, including BIM modeling, electronic document management systems, cloud technologies and artificial intelligence, are proposed. The concept of a multi-level management system for design and estimate documentation has been developed, taking into account the specifics of the construction industry. Practical recommendations on the implementation of the proposed solutions and assessment of their economic efficiency are presented. The results of the study are of practical importance for construction organizations of various scales seeking to optimize documentation management processes.*

Keywords: *design and estimate documentation, construction organization, electronic document management, BIM technologies, information security, digitalization of construction, documentation management, cloud technologies, artificial intelligence, archiving system.*

НЕФТЯНАЯ ПРОМЫШЛЕННОСТЬ

ШАРОНОВ Артем Викторович
студент, Астраханский государственный технический университет, Россия, г. Астрахань

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ НА РОССИЙСКИХ ПРЕДПРИЯТИЯХ В УСЛОВИЯХ САНКЦИОННЫХ ОГРАНИЧЕНИЙ

Аннотация. *В современном мире эффективность и конкурентоспособность предприятий во многом определяются уровнем внедрения автоматизированных систем управления (АСУ). Особенно актуально это для российских предприятий, сталкивающихся с усложнившимися условиями деятельности в условиях санкционных ограничений. Ограничения, введённые международными партнёрами, существенно повлияли на доступ к технологиям, оборудованию и программному обеспечению, что требует поиска новых решений для обеспечения стабильной работы и развития предприятий. В данной статье рассматриваются особенности внедрения и эксплуатации автоматизированных систем управления на российских предприятиях в условиях санкционных ограничений, а также анализируются возможные направления их развития и адаптации к новым реалиям.*

Ключевые слова: *программный аппаратный комплекс, автоматизация, объекты критической информационной инфраструктуры.*

Введение

Автоматизация технологических процессов является решающим фактором в повышении производительности труда и улучшении качества выпускаемой продукции. Для нефтегазового комплекса автоматизация имеет особое значение, так как он является одной из ведущих отраслей Российской Федерации и в значительной степени определяет её экономическое развитие. В настоящее время одним из приоритетных и перспективных направлений научно-технологического развития РФ является «переход к передовым цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших объемов данных, машинного обучения и искусственного интеллекта». С целью реализации данной концепции во многих отраслях промышленности внедряются современные системы автоматизированного управления производством и системы поддержки принятия решений при осуществлении технологических процессов. В сфере добычи углеводородного сырья такие системы высоко востребованы в процессах обслуживания и управления нефтегазодобывающими скважинами, нефтепроводами и другими технологическими объектами.

Но в современном мире Российская Федерация столкнулась с санкционными ограничениями, которые могут препятствовать технологическому развитию и безопасности предприятий. Поэтому с 1 сентября 2024 года в России вступают в силу Правила перехода субъектов критической информационной инфраструктуры на преимущественное применение доверенных программно-аппаратных комплексов (ПАК) на принадлежащих им значимых объектах критической информационной инфраструктуры (КИИ) [1].

Переход на доверенные ПАК

Переход на доверенные программные и аппаратные комплексы в субъектах критической инфраструктуры Российской Федерации является важной частью реализации мер по обеспечению информационной безопасности и независимости от иностранных технологий. В рамках национальных стратегий по защите критической инфраструктуры и реализации требований законодательства, таких как Федеральный закон № 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации» [2], осуществляется переход на отечественные

решения, соответствующие высоким стандартам надежности и безопасности.

Ключевые аспекты перехода включают:

- Замещение иностранных программных и аппаратных решений на отечественные аналогичные продукты, сертифицированные по российским стандартам.
- Создание и внедрение систем управления безопасностью, соответствующих требованиям российского законодательства.
- Обеспечение совместимости и интеграции новых комплексов с существующими инфраструктурными объектами.

Примеры успешных переходов:

- Московский метрополитен – осуществил переход на отечественные системы управления и безопасности, что повысило устойчивость к киберугрозам и обеспечило независимость от иностранных поставщиков.
- Российские энергосистемы – ряд субъектов энергетической отрасли внедрили отечественные системы автоматизации и телемеханики, такие как решения на базе российского программного обеспечения и аппаратуры, что повысило безопасность и контроль.
- Государственные органы и ведомства – многие федеральные и региональные структуры заменили иностранные решения на российские аналоги, что подтверждается сертификациями и успешной эксплуатацией.

Трудности при переходе на доверенные ПАК

При переходе нефтегазовых предприятий на доверенные программно-аппаратные комплексы (например, системы с повышенной безопасностью и доверенной вычислительной средой) они могут сталкиваться со следующими сложностями:

Высокие затраты на внедрение и модернизацию:

- приобретение новых систем требует значительных финансовых инвестиций.
- необходимость обновления инфраструктуры и оборудования.

Сложности интеграции с существующими системами:

- несовместимость новых доверенных комплексов с устаревшими системами и протоколами.
- необходимость разработки специальных интерфейсов и адаптеров.

Квалификационные требования персонала:

- – необходимость обучения сотрудников работе с новыми системами.
- – привлечение специалистов, обладающих знаниями в области доверенных вычислений и информационной безопасности.

Обеспечение непрерывности производственных процессов:

- риск простоя оборудования и систем во время внедрения.
- необходимость планирования поэтапного перехода.

Соответствие нормативным требованиям и стандартам:

- необходимость подтверждения соответствия новым системам требованиям безопасности, промышленной безопасности и экологическим стандартам.
- прохождение аудитов и сертификаций.

Обеспечение информационной безопасности и управления рисками:

- обеспечение защиты от кибератак и несанкционированного доступа в условиях повышенных требований к безопасности.
- управление сложными ключами и сертификатами.

Культурные и организационные изменения:

- изменение рабочих процессов и процедур.
- необходимость внедрения новых правил и политик безопасности.

Технические ограничения и сложности разработки:

- разработка или адаптация программного обеспечения под новые доверенные платформы.
- обеспечение совместимости и масштабируемости.

Экспертами был отмечен высокий потенциал российских ИТ-разработчиков.

При этом респонденты указали и на ограничения, которые есть у отечественных вендоров: отсутствие собственной компонентной базы, недостаточные вложения в R&D, высокие цены и длинные сроки поставки. Закрытость, проприетарность отечественных решений также является существенным ограничением.

Одной из главных проблем является недостаточная зрелость и апробированность отечественных решений.

Эти сложности требуют комплексного подхода, тщательного планирования и тесного взаимодействия между специалистами по информационной безопасности, инженерными службами и руководством предприятий.

Вывод

Несмотря на трудности реализации данного процесса, переход на доверенные комплексы в РФ является реализуемым и уже реализован в отдельных сферах, что свидетельствует о стратегическом курсе на обеспечение национальной безопасности и технологической независимости.

Литература

1. Постановление правительства РФ «О порядке перехода субъектов критической информационной инфраструктуры РФ на преимущественное применение доверенных программно-аппаратных комплексов (ПАК) на принадлежащих им значимых объектах критической информационной инфраструктуры РФ» от 14.11.2023 № 1912.

2. № 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации» от 26.07.2017.

SHARONOV Artyom Viktorovich
Student, Astrakhan State Technical University, Russia, Astrakhan

AUTOMATED CONTROL SYSTEMS AT RUSSIAN ENTERPRISES UNDER SANCTIONS RESTRICTIONS

Abstract. *In the modern world, the efficiency and competitiveness of enterprises are largely determined by the level of implementation of automated control systems (ACS). This is especially true for Russian enterprises facing complicated operating conditions under sanctions restrictions. The restrictions imposed by international partners have significantly affected access to technology, equipment and software, which requires the search for new solutions to ensure stable operation and development of enterprises. This article examines the specifics of the implementation and operation of automated control systems at Russian enterprises under the conditions of sanctions restrictions, as well as analyzes possible directions for their development and adaptation to new realities.*

Keywords: *software hardware complex, automation, critical information infrastructure facilities.*

Актуальные исследования

Международный научный журнал
2025 • № 20 (255)
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 26.05.2025г. Формат 60×90/8. Тираж 500 экз. Цена свободная.
308010, г. Белгород, пр-т Б. Хмельницкого, 135, офис 40