

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Институт права, социального управления и безопасности
Кафедра информационной безопасности в управлении

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ: СОВРЕМЕННОСТЬ И ПЕРСПЕКТИВЫ

Сборник статей
Всероссийской студенческой научно-практической
конференции с международным участием
24 апреля 2025 г.



Ижевск
2025

ISBN 978-5-4312-1286-4

© ФГБОУ ВО «Удмуртский
государственный университет», 2025
© Авторы статей, 2025

УДК 004:621.31(063)
ББК 16.84я431+31.2-057я431
О-136

Рекомендовано к изданию редакционно-издательским советом УдГУ

Рецензенты: канд. техн. наук, доцент, доцент каф. теплоэнергетики ФГБОУ ВО «Удмуртский государственный университет» **Е.М. Борисова;**

канд. техн. наук, доцент, доцент каф. электротехники, электрооборудования и электроснабжения ФГБОУ ВО «Удмуртский государственный аграрный университет» **Т.А. Широбокова.**

Научный редактор: Т.Н. Стерхова, канд. техн. наук, доцент, доцент каф. информационной безопасности в управлении ИПСУБ ФГБОУ ВО «Удмуртский государственный университет».

О-136 Обеспечение информационной безопасности в электроэнергетике: современность и перспективы : сб. ст. студ. Всерос. науч.-практ. конф. с междунар. участием (24 апр. 2025 г.) / науч. ред. Т.Н. Стерхова. – Ижевск : Удмуртский университет, 2025. – 1 DVD-R (4,4 Мб). – Текст: электронный.

Сборник содержит статьи студентов – участников Всероссийской научно-практической конференции «Обеспечение информационной безопасности в электроэнергетике: современность и перспективы», проведенной Институтом права, социального управления и безопасности Удмуртского государственного Университета 24 апреля 2025 года. В статьях рассматриваются актуальные вопросы обеспечения информационной безопасности в электроэнергетике.

Минимальные системные требования:

Celeron 1600 Mhz; 128 Мб RAM; WindowsXP/7/8 и выше; разрешение экрана 1024×768 или выше; программа для просмотра pdf

ISBN 978-5-4312-1286-4

© ФГБОУ ВО «Удмуртский
государственный университет», 2025
© Авторы статей, 2025

**Обеспечение информационной безопасности в электроэнергетике:
современность и перспективы**

Сборник статей Всероссийской студенческой научно-практической
конференции с международным участием 24 апреля 2025 г.

Подписано к использованию 10.09.2025
Объем электронного издания 4,4 Мб, тираж 10 экз.
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел. : +7(3412)916-364 E-mail: editorial@udsu.ru

СОДЕРЖАНИЕ

Абрарова А.Р., Косянчук Д.И., Трофимов В.А. Современные методы обнаружения и анализа уязвимостей в компьютерных системах: технологии и практика	5
Афанасьева А.А. Проектирование web-сайта и игры в сфере информационной безопасности	9
Белоусов А.Н., Полетаев Д.Е. Защита информации от утечки по системам заземления	14
Бычков Н.А. Использование нейросети для составления отчета по курсу «Технология программирования»	19
Васильченко Д.А., Фролов М.А. Исследование усилителей переменного напряжения, построенных на операционных усилителях	36
Власенко И.П. Способы защиты от утечки информации по цепям электропитания средств вычислительной техники	44
Гарафиева В.Р. Внедрение концепции BYOD в политику безопасности организации.....	50
Егоров В.А. Обеспечение защиты данных при проведении тестирования средствами Google Форм	53
Желнин А.М., Новосельских Д.А. Создание приложения для оповещения граждан о правонарушениях	57
Кагарманов А.Р., Исупов Р.С. Исследование LC-автогенератора гармонических колебаний	61
Коноплёв А.А. Проведение испытаний силовых кабелей для защиты информации.....	66
Кутергин Д.С., Шамшурина А.А. Разработка программного средства для автоматизации проектирования цифровых фильтров в системах информационной безопасности	69
Павлова З.Д. Информационная безопасность в цифровых подстанциях	72
Пархачёва А.А. Программа моделирования очереди по распределению Пуассона	77
Пархачёва А.А. Современное состояние безопасности информационных систем в электроэнергетике разных стран.....	80
Поносова А.Д., Рахимов И.Э. Защита информации от утечки по цепям электропитания	84
Пославская В.Я. Автоматизация процедуры обработки экспертных решений в ОВД.....	88

Пославская В.Я. Проектирование сегмента сети связи специального назначения для подразделений органов внутренних дел.....	92
Потемкина Т.М. Требования, регламентирующие процесс управления уязвимостями	96
Распутин И.Е. Комплексная защита сетей электроснабжения	99
Старков В.М. Разработка программы для расчета выпрямителя	101
Тумашов Е.Н. Проектирование энергоэффективной калориферной системы отопления для производственных предприятий с учетом защиты информации от утечки по техническим каналам	105
Хасанов И.Р., Лазарева А.П. Сравнение методов машинного обучения для диагностики силовых трансформаторов	109
Хозеев И.И. Автоматизация обработки инцидентов информационной безопасности	114
Шилов Д.А. Эволюция DevOps (DevSecOps) – от виртуализации к контейнерной оркестрации с помощью Docker и Kubernetes	116

**Абрарова Аделия Ралифовна,
Косянчук Дарья Игоревна,
Трофимов Владислав Александрович,**

*обучающиеся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры
информационной безопасности в управлении Удмуртского
государственного университета,
г. Ижевск*

СОВРЕМЕННЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ И АНАЛИЗА УЯЗВИМОСТЕЙ В КОМПЬЮТЕРНЫХ СИСТЕМАХ: ТЕХНОЛОГИИ И ПРАКТИКА

Современные компьютерные системы играют ключевую роль в функционировании организаций и отраслей экономики. С ростом их значимости увеличивается количество угроз, связанных с уязвимостями в программном обеспечении. Уязвимости могут привести к утечке данных, сбоям и финансовым потерям. Автоматизация выявления и анализа уязвимостей позволяет сократить время реагирования на инциденты и повысить уровень информационной безопасности.

Цель исследования – изучить современные методы автоматизированного обнаружения и анализа уязвимостей в компьютерных системах с акцентом на практическое применение и использование базы данных ФСТЭК.

Задачи – изучение теоретических основ, обзор современных технологий и подходов к автоматизированному анализу уязвимостей, оценка роли и структуры базы данных уязвимостей ФСТЭК, исследование её возможностей как инструмента для повышения уровня информационной безопасности и обеспечения киберзащиты в российской практике.

Теоретические основы автоматизированного обнаружения и анализа уязвимостей. Уязвимость – это слабое место или дефект в программном обеспечении (ПО) или аппаратном обеспечении, которое может быть использовано злоумышленниками для несанкционированного доступа, модификации или разрушения данных, а также для нарушения нормальной работы системы. Уязвимости могут проявляться в разных формах, включая ошибки в коде, небезопасные настройки, устаревшие протоколы или алгоритмы, а также другие дефекты, которые могут быть использованы для осуществления атак. Важно

отметить, что уязвимости могут присутствовать как в известных программных продуктах, так и в новых, еще не тестированных системах. В 2008 году база данных CVE (Common Vulnerabilities and Exposures) зарегистрировала значительное количество уязвимостей, что стало индикатором возрастающей угрозы информационной безопасности и подчеркнуло необходимость разработки методов для быстрого обнаружения и устранения уязвимостей¹.

Одной из ключевых задач в области информационной безопасности является классификация уязвимостей, что помогает систематизировать угрозы, а также эффективно управлять рисками безопасности. Уязвимости могут быть классифицированы по различным признакам:

1. Структурные уязвимости – это дефекты, связанные с проектированием системы или архитектуры, которые могут проявляться на уровне протоколов, алгоритмов или взаимодействия компонентов. Примером является неправильная реализация криптографических алгоритмов, которые могут быть расшифрованы злоумышленниками при наличии уязвимости в самой системе.

2. Эксплуатационные уязвимости – это ошибки или недочеты, возникающие в процессе эксплуатации системы, чаще всего из-за недостатков в использовании программного обеспечения. К этому типу относятся ошибки, возникающие в результате неверных действий пользователей, администраторов или других сторон, неправильно настраивающих систему. Это может быть связано с неправильной настройкой доступа, использованием слабых паролей или несанкционированным доступом через публичные сервисы.

Кроме того, можно выделить другие категории, такие как конфигурационные уязвимости (связаны с неверными настройками системы) и интерфейсные уязвимости (связаны с недостаточной безопасностью взаимодействия между различными системами).

Исследования показывают, что значительное количество инцидентов в области безопасности связано с уже известными уязвимостями, которые не были своевременно устранены или исправлены. Это подчеркивает важность регулярного обновления системы, внедрения патчей и улучшений безопасности. Согласно данным различных исследований, большинство атак происходят именно через эксплуатацию известных уязвимостей, что делает управление ими критически важным для защиты информации².

¹ *Евтеев Д.* Статистика уязвимостей Web-приложений за 2008 год: [Электронный ресурс]. URL: <http://www.ifap.ru>. С. 6.

² *Марков А.С., Фадин А.А.* Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. INSIDE, 2013. С. 1–3.

Роль базы данных уязвимостей. БДУ ФСТЭК – одна из крупнейших российских баз данных, содержащая значительный объем информации об уязвимостях, и в 2024 году она была значительно расширена. База включает более 50 тыс. записей с подробными описаниями, степенью критичности и рекомендациями, предоставляя централизованную, структурированную информацию, необходимую для эффективного управления безопасностью. ФСТЭК регулярно обновляет базу данных и поддерживает её совместимость с международными стандартами, включая CVE и CVSS. Это способствует своевременному обмену данными о киберугрозах и позволяет учитывать, как отечественные, так и глобальные риски.

БДУ ФСТЭК активно используется в автоматизированных системах мониторинга, включая корпоративные и государственные решения по информационной безопасности. Его интеграция с анализаторами и сканерами уязвимостей (такими как *MaxPatrol*, *Security Vision*, *Positive Technologies* и др.) позволяет проводить регулярные аудиты безопасности, автоматически оценивать риски на основе актуальных данных, формировать отчётность в соответствии с требованиями регуляторов.

Современные методы автоматизированного анализа. Анализ уязвимостей в современных условиях требует скорости, точности и системности. В связи с этим широко применяются автоматизированные подходы, позволяющие оперативно выявлять угрозы и снижать риски.

На смену традиционному ручному анализу приходит автоматизированный, что обусловлено постоянным ростом числа регистрируемых уязвимостей. В условиях, когда ежегодно регистрируется более 25 тысяч новых угроз (по данным NVD), вручную обрабатывать такие объемы информации становится неэффективно. Автоматизация процесса позволяет значительно ускорить выявление уязвимостей, повысить точность анализа и оперативность принятия решений, что делает её неотъемлемой частью современных систем информационной безопасности³.

Наиболее распространены статический, динамический и гибридный методы. Статический анализ позволяет находить уязвимости на этапе разработки, то есть в коде (эффективен для известных уязвимостей), динамический – в процессе работы системы (для новых и специфичных угроз). Гибридный подход

³ *Киргизбаев С.П., Киргизбаев В.П., Бутин А.А.* Применение сканеров уязвимостей для обнаружения потенциальных угроз информации в корпоративной сети и анализа её защищённости. Статья. Иркутск : Иркутский гос. университет путей сообщения, 2023.

объединяет преимущества обоих и обеспечивает наиболее полное покрытие, сокращая время обработки⁴.

Современные технологии включают машинное обучение, обработку естественного языка и семантический поиск. Автоматизация сокращает время обнаружения угроз существенно⁵. В отечественной практике применяются решения, такие как RedCheck, ScanOVAL и модули, использующие данные БДУ ФСТЭК. Они позволяют интегрировать национальную базу уязвимостей в системы контроля защищённости.

Важной тенденцией является интеграция модулей анализа уязвимостей с системами управления событиями безопасности (SIEM), что обеспечивает централизованный мониторинг и автоматическую корреляцию инцидентов. SIEM-системы представляют собой инструменты, которые собирают и анализируют события безопасности из различных источников в реальном времени, такие как журналы серверов, сетевых устройств и приложений. Когда модули анализа уязвимостей интегрируются с SIEM, это позволяет собирать данные о возможных угрозах из различных источников, таких как базы данных уязвимостей (например, БДУ ФСТЭК, CVE, EPSS) и инструменты сканирования.

Централизованный мониторинг дает возможность автоматически обрабатывать и классифицировать угрозы в одном месте, что ускоряет выявление инцидентов и сокращает время реагирования. Автоматическая корреляция инцидентов, в свою очередь, позволяет системе анализировать связку различных событий, определяя возможные угрозы на основе комбинации признаков. Например, если сканер уязвимостей обнаруживает слабое место в системе, а система SIEM фиксирует подозрительное поведение, интеграция этих данных позволяет оперативно сформировать полную картину инцидента и назначить приоритетные меры реагирования.

Автоматизация анализа позволяет значительно сократить время реагирования на инциденты и повысить эффективность информационной безопасности, особенно в корпоративных инфраструктурах.

⁴ Совершенствование методологии и организации научных исследований в целях развития общества : сборник статей Международной научно-практической конференции (12 апреля 2022 г., г. Уфа). Уфа : OMEGA SCIENCE, 2022. С. 23.

⁵ Павлычев А.В., Стародубов М.И., Галимов А.Д. Использование алгоритма машинного обучения Random Forest для выявления сложных компьютерных инцидентов // Вопросы кибербезопасности. 2022. № 5 (51). С. 74–81.

Афанасьева Анастасия Андреевна,

обучающаяся 4 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры

информационной безопасности в управлении Удмуртского

Государственного Университета,

г. Ижевск

ПРОЕКТИРОВАНИЕ WEB-САЙТА И ИГРЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современных условиях, когда киберугрозы становятся все более изощренными, проектирование веб-сайтов и компьютерных игр в области информационной безопасности приобретает особую актуальность. Статья рассматривает ключевые аспекты создания таких цифровых продуктов, дает рекомендации по их защите и обеспечивает пользователей безопасным взаимодействием с информацией.

Веб-сайты и игры, посвященные информационной безопасности, представляют собой перспективное направление в решении этой проблемы. Они позволяют в увлекательной форме обучать пользователей основным правилам безопасности, демонстрировать последствия небрежного отношения к личным данным и прививать навыки распознавания киберугроз. Создание качественных и эффективных веб-сайтов и игр в этой сфере является важной задачей, направленной на повышение осведомленности и защиту пользователей в интернете.

При проектировании веб-сайтов, особенно тех, что содержат чувствительную информацию, следует учитывать такие принципы, как минимизация привилегий, шифрование данных, защита от атак, таких как SQL-инъекции и Cross-Site Scripting (XSS). В контексте игрового дизайна важным аспектом является обеспечение безопасности игровых сессий и предотвращение мошенничества.

Удобный и интуитивно понятный интерфейс не только повышает пользовательский опыт, но и снижает вероятность ошибок, которые могут привести к нарушениям безопасности. Применение принципа "безопасность по умолчанию" (security by default) гарантирует, что пользователи получают защищенные настройки, а не настройки, требующие дополнительной конфигурации.

Веб-сайт должен быть простым и удобным в навигации, чтобы дети могли легко находить нужную информацию и проходить задания. Основные разделы сайта могут включать:

1. Главная страница: Приветствие, краткая информация о сайте и его целях, ссылки на основные разделы.

2. Игровой раздел: Основная часть сайта, где дети могут проходить различные уровни игры, учась распознавать угрозы и правильно реагировать на них. Игра может быть основана на квестах, где пользователи будут решать задачи, сталкиваясь с различными ситуациями, связанными с безопасностью в Интернете.

3. Учебные материалы: Этот раздел будет содержать статьи, видеоролики и интерактивные уроки по основам безопасности в интернете. Материалы должны быть развлекательными и информативными.

4. Форум: Площадка для общения, где дети могут задавать вопросы, делиться опытом и получать помощь. Раздел может быть модератором, чтобы избежать нежелательных взаимодействий.

5. Тестирование и достижения: Дети могут проходить тестирование по пройденному материалу и получать достижения за успешное выполнение заданий, что будет мотивировать их продолжать обучение.

Дизайн веб-сайта представлен на рис. 1, он должен быть красочным и привлекающим внимание. Использование мультяшных персонажей и анимации может сделать обучение более увлекательным. Важно также обеспечить доступность для детей с ограниченными возможностями, адаптировав контент под различные потребности.

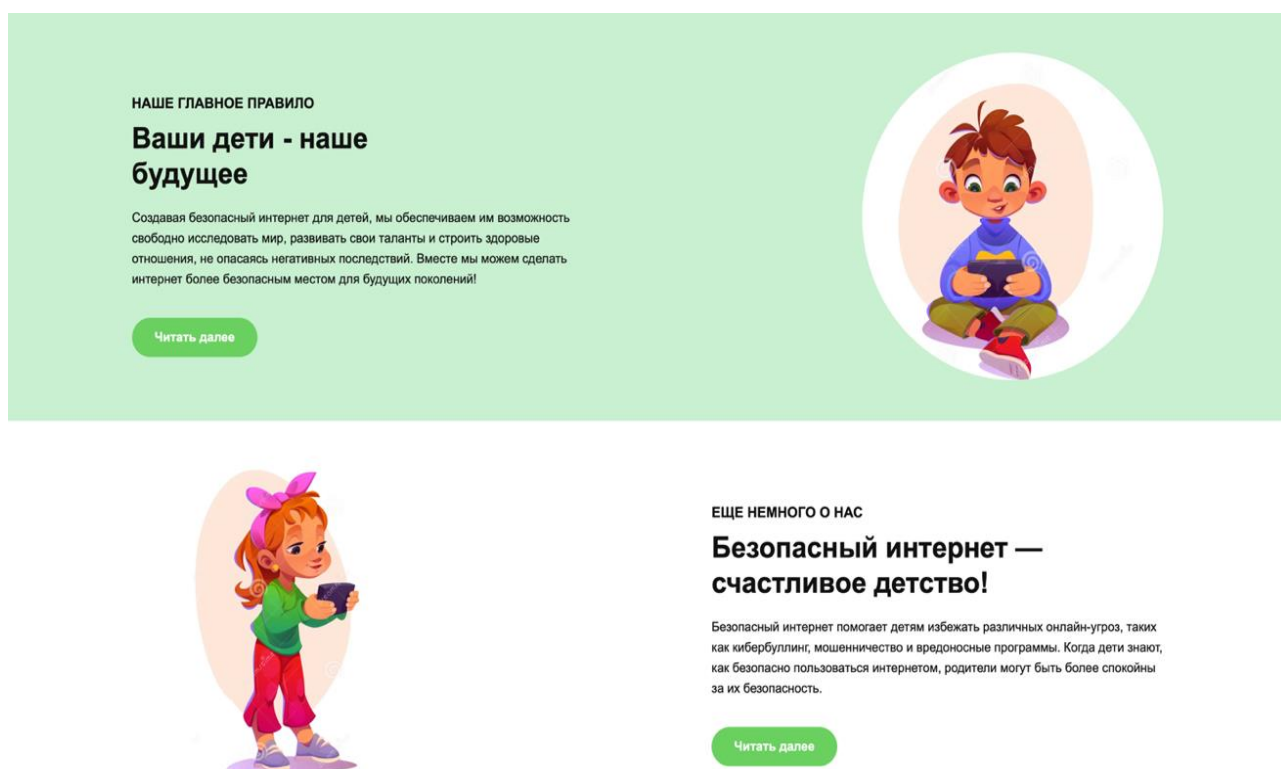


Рис. 1.

Авторизация в игре – это важный процесс, который обеспечивает безопасность учетных записей пользователей и позволяет сохранить прогресс в игре, представлен на рис. 2. Заголовок "Вход в игру" расположен в верхней части белого прямоугольного блока с закругленными углами.

Под заголовком расположены два поля для ввода данных:

- "Имя пользователя";
- "Пароль".

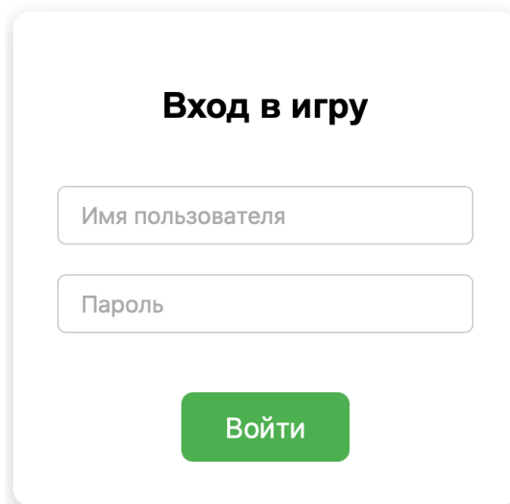


Рис. 2.

Общий стиль оформления лаконичный и современный. Используется белый фон и простой шрифт. Никаких дополнительных элементов дизайна или иллюстраций не присутствует. Форма предназначена для ввода учетных данных и входа в игру.

1. Пользователь вводит свои учетные данные (логин и пароль) в соответствующие поля. После нажатия кнопки "Войти" происходит проверка введенных данных на стороне сервера.

2. Сервер проверяет, существуют ли указанные логин и пароль в базе данных. Если данные верны, пользователю предоставляется доступ к игре. В противном случае отображается сообщение об ошибке с предложением повторить попытку.

3. Игроку может быть предложено сохранить свои учетные данные для автоматического входа при следующем запуске игры (опция "Запомнить меня").

4. Пользователь может выйти из своей учетной записи в любой момент, нажав кнопку "Выйти", что завершает текущую сессию и возвращает его на экран входа.

Процесс авторизации является важным элементом игрового опыта, обеспечивая безопасность и персонализацию для каждого игрока. Правильная реализация этого процесса помогает создать доверительную атмосферу и способствует вовлечению пользователей в игру.

При запуске игры, на начальной странице, размещено приветствие в центре экрана, который содержит яркий и акцентный шрифт, при этом легко читаемый, расположенный на зеленом фоне, который помогает создать дружелюбную и успокаивающую атмосферу, что делает его дружелюбным для детской аудитории. Текст приветствия содержит следующее: «Привет, защитник информации! Готов стать супергероем в мире кибербезопасности?», это сообщение не только приветствует пользователей, но и сразу погружает их в тематику игры, подчеркивая, что они будут обучаться важным навыкам и получать новые знания. Фон страницы оформлен в спокойном цвете, не создающим ассоциации опасности. Кнопка «Начать игру» явно выделена на странице, она отличается по цвету от основного и имеет достаточно большой размер, для того чтобы её было легко заметить и нажать. Такой простой, но привлекательный и функциональный дизайн начальной страницы позволит пользователям сразу погрузиться в атмосферу игры.

Главным героем является милый котенок, за которого играет пользователь, представлен на рис. 3. Игра представляет собой увлекательное и познавательное приключение, направленное на обучение основам безопасного поведения в сети «Интернет». Игроку предстоит управлять котенком, который прыгает по ступенькам – заданиям, чтобы продвигаться вперед к новым увлекательным уровням. Каждая ступенька соответствует определенному вопросу, касающемуся различных аспектов информационной безопасности.

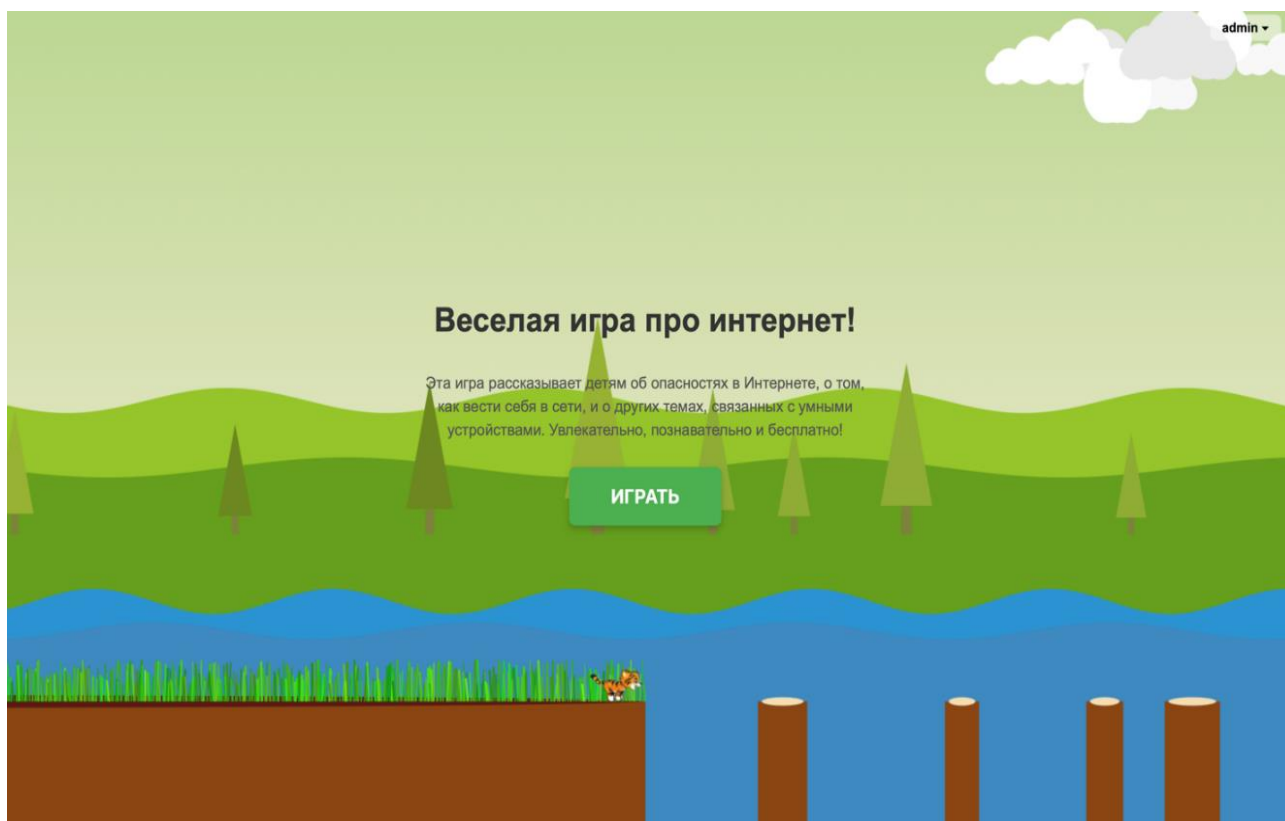


Рис. 3.

В начале игры котёнок стоит на первом уровне, окруженный ярким и красочным фоном, которые создают дружелюбную атмосферу игры. Как только игрок нажимает кнопку «Играть», котенок начинает прыгать по ступенькам, где появляется вопрос. Если игрок отвечает неправильно, вопрос повторяется, и котенок остается на том вопросе, на котором он был, что создает чувство важности правильного выбора, функционал представлен на рис. 8. Таким образом, дети учатся совершать ошибки и исправлять их, что является важным аспектом обучения. Если ответ на вопрос оказывается верным, котёнок с радостью прыгает дальше на следующую ступеньку, сталкиваясь с новым вопросом.

По мере продвижения по уровням сложность вопросов увеличиваются и меняется тема вопросов. Всего представлено 4 уровня по таким темам, как:

1. Основы интернет-безопасности.

2. Социальные сети. Почему не стоит делиться личной информацией с незнакомцами?

3. Игровая среда.

4. Моё свободное время в Интернете.

Игра по интернет-безопасности предназначена для достижения следующих целей:

- предоставить пользователям (детям и подросткам) знания и навыки, необходимые для безопасного использования интернета;

- сделать пользователей более внимательными и осторожными в интернете. Научить их критически оценивать информацию, не доверять подозрительным ссылкам и сообщениям, а также защищать свою личную информацию;

- сформировать у пользователей устойчивые привычки безопасного поведения в интернете. Превратить соблюдение правил безопасности из формальности в автоматическую реакцию;

- снизить вероятность стать жертвой киберпреступников и мошенников. Защитить пользователей от финансовых потерь, кражи личных данных и других негативных последствий;

- способствовать формированию более безопасной онлайн-среды для всех пользователей.

**Белоусов Андрей Николаевич,
Полетаев Денис Евгеньевич,**

обучающиеся 2 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

*Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры
информационной безопасности в управлении Удмуртского
государственного университета,
г. Ижевск*

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО СИСТЕМАМ ЗАЗЕМЛЕНИЯ

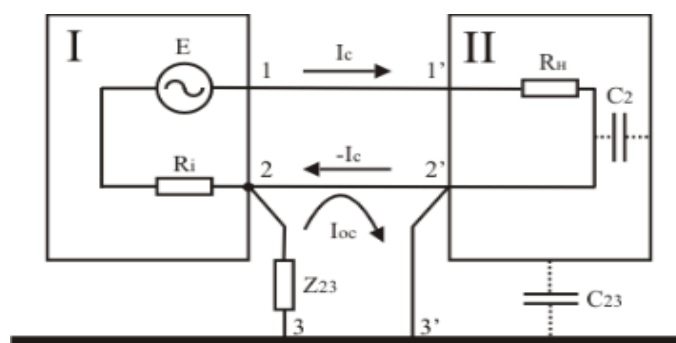
В современных информационных системах защита данных от утечки является одной из ключевых задач. Одним из потенциальных каналов утечки информации являются системы заземления, которые, несмотря на свою важность для электробезопасности и снижения помех, могут стать источником опасных сигналов. В данной статье рассматриваются механизмы утечки информации через заземляющие цепи, а также методы защиты от таких утечек.

1. Основные принципы заземления: заземление представляет собой преднамеренное подключение устройства к заземляющему элементу, осуществляемое с помощью системы проводящих элементов и соединений. Основные функции заземления включают:

- 1) обеспечение электробезопасности;
- 2) снижение электромагнитных помех;
- 3) защиту оборудования от перенапряжений.

Заземление экранирующих поверхностей способствует уменьшению электромагнитных наводок и является частью общей экранирующей системы. *Проводящие элементы обеспечивают путь для обратных токов в сигнальных и питающих цепях*⁶.

2. Механизмы утечки информации через заземление



⁶ О защите информации через системы заземления: теоретические основы // StudFile.
URL: <https://studfile.net/preview/5970814/page:21/> (дата обращения: 28.04.2025).

2.1. Образование заземляющих контуров

Одной из причин утечки информации является наличие заземляющих контуров, возникающих при неправильном подключении оборудования. Если два устройства соединены через общий заземляющий проводник, внешнее электромагнитное поле может индуцировать в этом контуре ток, создающий опасные наводки. Даже при отсутствии прямого соединения контур может замыкаться через:

- Паразитные ёмкости между цепями и корпусом.
- Сопротивление грунта.
- Общие заземляющие шины.

2.2. Утечка из-за сопротивления заземляющих проводников

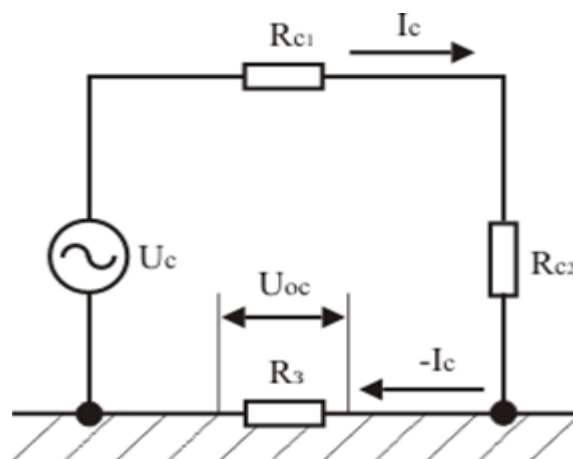
Конечное сопротивление заземляющих проводников приводит к падению напряжения:

$$U_{oc} = I_{oc} \cdot Z_{23}$$

Если заземляющий проводник используется как обратный проводник для сигнальной цепи, напряжение на нагрузке может изменяться из-за падения напряжения на сопротивлении заземления:

$$U_{нагр} = U_c - I \cdot R_3$$

Это создаёт риск перехвата информации через заземляющую цепь⁷.

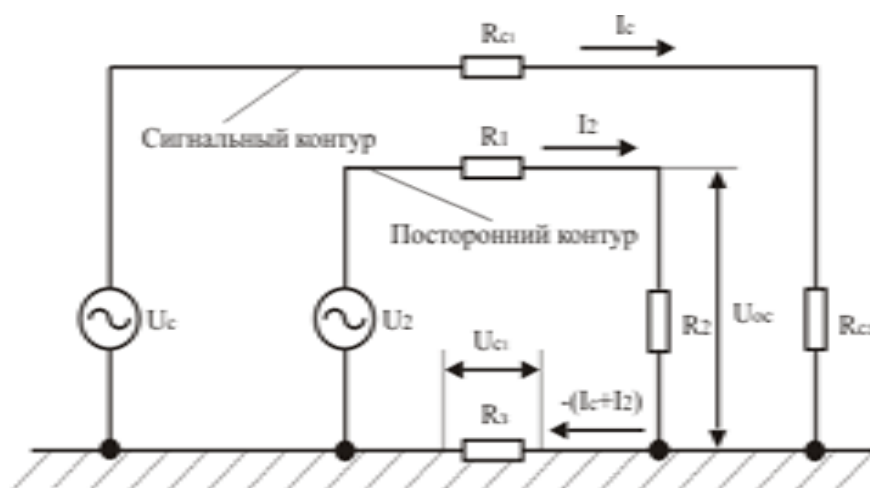


2.3. Утечка по общей заземляющей цепи

Когда несколько устройств используют одну заземляющую шину, ток от одного устройства может создавать помехи в другом. Падение напряжения на общем сопротивлении заземления приводит к взаимному влиянию цепей⁸ (см. схему на стр. 16).

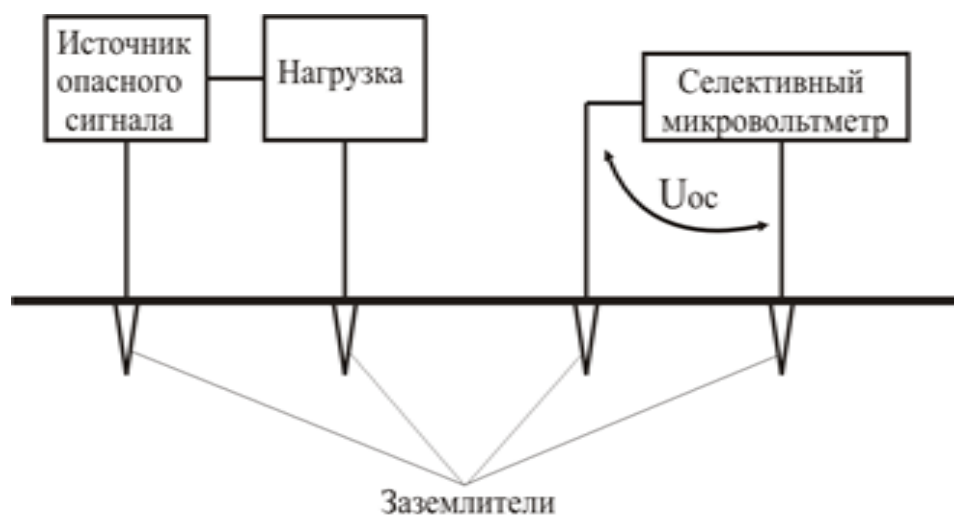
⁷ О защите информации через системы заземления: теоретические основы // StudFile. URL: <https://studfile.net/preview/5970814/page:21/> (дата обращения: 28.04.2025).

⁸ Крылов В.В. Теоретические основы электротехники. Москва : Юрайт, 2021. 480 с.



2.4. Распространение сигнала через грунт

Электрическое поле заземлителя может распространяться через грунт, создавая канал утечки. Хотя магнитная составляющая быстро затухает, электрическая может быть перехвачена с помощью дополнительных заземляющих электродов⁹.



3. Методы защиты от утечки информации через заземление

3.1. Раздельное заземление

Для минимизации паразитных контуров рекомендуется применять раздельное заземление:

- Силовое заземление – для питания оборудования.
- Сигнальное заземление – для информационных цепей.
- Защитное заземление – для электробезопасности.

3.2. Использование экранированных кабелей

⁹ Кузнецов С.В. Защита информации в автоматизированных системах. Москва : Форум, 2018. 288 с.

Экранирование сигнальных линий и их заземление в одной точке снижает влияние наводок. Важно избегать образования контуров при подключении экранов¹⁰.

3.3. Гальваническая развязка

Применение оптронов, трансформаторов и других средств гальванической развязки исключает протекание токов утечки через заземляющие цепи¹¹.

3.4. Контроль сопротивления заземления

Регулярные измерения сопротивления заземляющих устройств позволяют выявлять потенциальные каналы утечки¹².

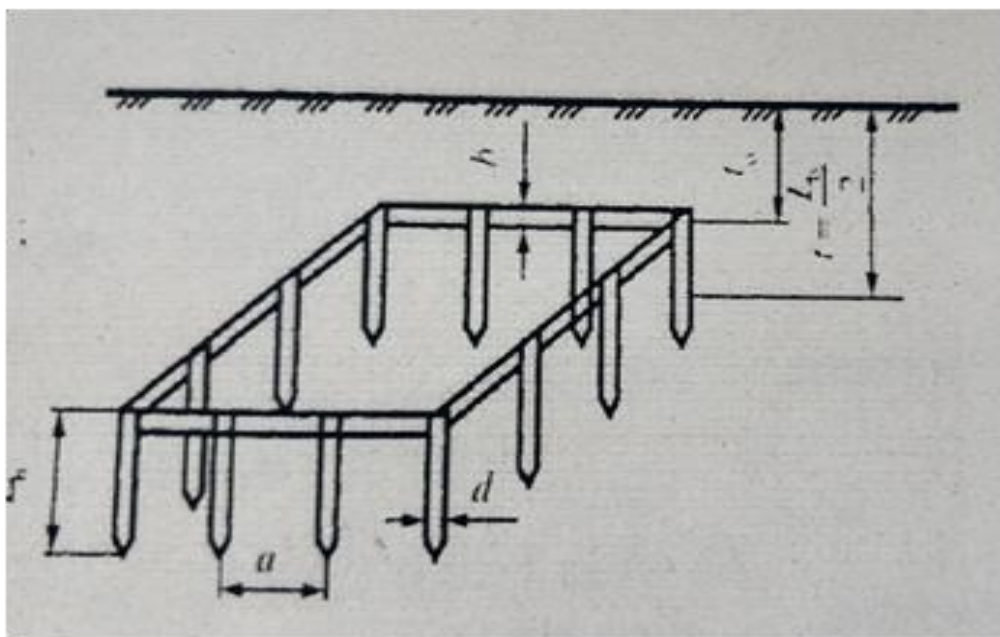
3.5. Защита от наводок через грунт

Использование изолированных заземляющих систем и экранированных помещений снижает риск перехвата сигналов через землю¹³.

4. Программа для расчёта сопротивления заземления (Python)

Для автоматизации расчётов разработана программа на Python, которая учитывает:

- Тип грунта (суглинок, песок, глина).
- Климатическую зону.
- Геометрические параметры заземлителей.



¹⁰ Смирнов А.Д. Заземление и молниезащита. Москва : Энергоатомиздат, 2016. 320 с.

¹¹ Рекомендации МЭК 61000-5-2 Электромагнитная совместимость (ЭМС). Международная электротехническая комиссия, 2019.

¹² ГОСТ Р 50571.5.54-2013 Электроустановки низковольтные. Часть 5-54. Заземляющие устройства, защитные проводники и защитные проводники уравнивания потенциалов. Москва : Стандартинформ, 2014.

¹³ Фёдоров В.В., Сергеев А.Б. Основы электробезопасности. Москва : Академия, 2020. 256 с.

Программа расчета заземления

Верхний слой грунта:	Песок влажный (400) ▾
Климатический коэффициент:	Климатическая зона I ▾
Нижний слой грунта:	Песок влажный (400) ▾
Количество верт. заземлителей:	3 вертикальных заземл. ▾
Глубина верхнего слоя грунта, H (м):	1
Длина вертикального заземлителя, L1 (м):	3
Глубина горизонтального заземлителя, h2 (м):	0.7
Длина соединительной полосы, L3 (м):	3
Диаметр вертикального заземлителя, D (м):	0.014
Ширина полки горизонтального заземлителя, b (м):	0.04

Выполнить расчет

Удельное электрическое сопротивление грунта (ом/м): 400.00
Сопротивление одиночного верт. заземлителя (ом): 231.98
Длина горизонтального заземлителя (м): 9.000
Сопротивление горизонтального заземлителя (ом): 311.68
Общее сопротивление растеканию электрического тока (ом): 61.956

Утечка информации через системы заземления является серьезной угрозой, особенно в высокозащищенных информационных системах. Для предотвращения таких утечек необходимо применять комплекс мер, включающий раздельное заземление, гальваническую развязку, экранирование и контроль паразитных параметров цепи. Правильная организация заземления не только обеспечивает электробезопасность, но и защищает конфиденциальные данные от несанкционированного доступа.

Мы составили программу на языке программирования Python для расчета сопротивления заземляющего устройства и конструкцию устройства, которую можно будет применять при изучении дисциплины «Электротехника» и «Основы электротехники и радиоэлектроники» студентами направлений «Информационная безопасность» и «Безопасность информационных технологий».

Бычков Никита Александрович,

обучающийся 1 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: М.М. Гайсин, старший преподаватель кафедры

информационной безопасности в управлении Удмуртского

государственного университета,

г. Ижевск

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТИ ДЛЯ СОСТАВЛЕНИЯ ОТЧЕТА ПО КУРСУ «ТЕХНОЛОГИЯ ПРОГРАММИРОВАНИЯ»

В статье рассматривается опыт применения языковой нейросетевой модели ChatGPT для автоматизации подготовки технической документации и отчёта по лабораторной работе в рамках курса «Технологии программирования». Цель исследования – оценить, насколько эффективно нейросеть справляется с задачами формализации спецификаций, генерации описаний функций, примеров ввода-вывода и теоретических разделов отчёта, а также выявить ограничения и необходимые меры по контролю качества получаемого материала.

Нейросеть ChatGPT представляет собой большую языковую модель, обученную на корпусе текстов различной тематики, способную воспринимать запросы на естественном языке и генерировать связные, структурированные тексты. В образовательном контексте она выступает в роли цифрового ассистента, который помогает студенту оформить спецификации программных модулей, пояснить работу функций и подготовить теоретические разделы отчёта.

В ходе работы были сформулированы следующие задачи нейросети:

1. *Структурирование спецификации программы:* описание модулей, входных и выходных данных, алгоритмов и обработка ошибок.

2. *Генерация подробных описаний функций:* пояснения ролей переменных, условий проверки и работы с файлами.

3. *Создание примеров тестовых данных:* образцы ввода-вывода для каждого модуля.

4. *Формулирование теоретической части:* введение, описания методик, выводы об эффективности подхода.

Полученный материал формировался на основе серии диалогов с ChatGPT, где запросы уточнялись до тех пор, пока не был достигнут требуемый формат и полнота информации. Это позволило сэкономить значительное время студента по сравнению с ручным набором и структурированием документации.

В первом запросе, для написания документации, были загружены код программы и Техническое задание. Сам запрос выглядел вот так: «По файлу тз.docx и программе из текстового документа напиши спецификацию. Спецификация содержит постановку задачи, анализ этой задачи и подробное описание действий, которые должна выполнять программа. В спецификации отражаются: состав входных, выходных и промежуточных данных; какие входные данные являются корректными и какие ошибочными; кто является пользователем программы и каким должен быть интерфейс; какие ошибки должны выявляться и какие сообщения должны выдаваться пользователю; какие ограничения имеет программа (например, программа расчета факториала может иметь ограничение по максимальному числу); все особые ситуации, которые требуют специального рассмотрения; какая документация должна быть подготовлена; перспективы развития программы.»

Результат данного запроса (текст слово в слово скопирован из ChatGPT):

СПЕЦИФИКАЦИЯ ПРОГРАММЫ

1. Постановка задачи

Разработать единое консольное приложение на языке C++, которое решает следующие 7 задач:

1. Вычисление начальной скорости и угла броска.

По заданным максимальной высоте подъёма (H) и дальности полёта (L) вычислить угол броска и начальную скорость с использованием известных физических формул.

2. Вычисление факториала.

Рассчитать факториал числа n (с ограничением, например, от 0 до 170), где $n!$ определяется как произведение всех натуральных чисел от 1 до n .

3. Вычисление момента порядка k .

Для заданного распределения случайной величины (ввод значений и соответствующих вероятностей) вычислить момент порядка k по формуле: $\mu_k = \sum (x_i^k \cdot P(x_i))$. Допускается ввод с клавиатуры, считывание из файла или генерация случайных чисел с равномерным распределением вероятностей.

4. Вычисление числа Фибоначчи.

По номеру числа (от 0 до 93) вычислить соответствующий член последовательности Фибоначчи (где $F(0)=0$, $F(1)=1$, а для $n \geq 2$ $F(n)=F(n-1)+F(n-2)$).

5. Расшифровка сообщения.

На основе справочного текста и набора пар индексов (номер строки и номер слова) сформировать итоговое сообщение. Ввод может осуществляться с клавиатуры или считываться из файла.

6. Анимация новогодней открытки.

Создать графическую анимацию с использованием библиотеки SFML, включающую смену изображений (Санта, олень, анимированные текстовые изображения и фон). Открытка должна содержать разноцветные надписи и информацию о разработчике.

7. Вычисление определителя матрицы 2×2 .

По заданной матрице 2×2 , элементы которой могут вводиться с клавиатуры, считываться из файла или генерироваться случайно, вычислить детерминант по формуле $\det = a \cdot d - b \cdot c$.

При этом программа должна быть циклической (позволять повторное выполнение выбранного модуля) и обеспечивать выбор способа ввода данных (с клавиатуры или из файла). Результаты вычислений выводятся на экран и записываются в файл (output.txt).

2. Анализ задачи

- **Объединение модулей:** Программа состоит из 7 независимых модулей, каждый из которых имеет контрольный пример, свою логику ввода/вывода и возможность записи результата в файл.

- **Защита от некорректного ввода:** Все модули используют специализированные функции (например, функцию `durak`) для проверки корректности вводимых данных. Это позволяет избежать ошибок, связанных с неверным типом данных или диапазоном значений.

- **Гибкость ввода:** Пользователь может выбирать способ ввода данных (с клавиатуры или из файла). Некоторые модули допускают генерацию случайных чисел (например, для модуля 3 и 7).

- **Универсальность:** Программа разработана таким образом, чтобы её можно было легко адаптировать для добавления новых задач или расширения функциональности.

- **Надёжность:** Программа содержит механизмы для обработки ошибок при чтении файлов, некорректном вводе, а также проверки соблюдения физических и математических ограничений (например, сумма вероятностей должна быть равна 1).

3. Подробное описание действий программы

Главное меню

- **Вывод меню:** При запуске программа выводит главное меню с вариантами выбора модуля (от 1 до 7) и опцией выхода (0).

- **Пользовательский выбор:** Пользователь выбирает номер модуля. При неверном выборе программа выводит сообщение об ошибке и повторно запрашивает ввод.

Модуль 1: Вычисление начальной скорости и угла броска

- **Ввод данных:**

- Способ ввода: с клавиатуры или из файла (например, input1.txt).
- Вводятся два параметра: максимальная высота подъёма (H) и дальность полёта (L).

- **Обработка данных:**

- Вычисляется тангенс угла по формуле: $\tan(\alpha) = (4 \cdot H) / L$.
- Определяется угол ($\alpha = \arctan((4 \cdot H) / L)$) и переводится в градусы.
- Вычисляется начальная скорость: $V = \sqrt{(g \cdot L / \sin(2 \cdot \alpha))}$, где $g = 9.81 \text{ м/с}^2$.

- **Вывод и запись результата:**

- Результаты выводятся на экран.
- При выборе записи – результат дописывается в файл output.txt.

Модуль 2: Вычисление факториала

- **Ввод данных:**

- Число n вводится с клавиатуры или считывается из файла (input2.txt).
- Допустимый диапазон – от 0 до 170.

- **Обработка данных:**

- Вычисление факториала через цикл.

- **Вывод и запись результата:**

- Результат выводится на экран и при необходимости записывается в файл output.txt.

Модуль 3: Вычисление момента порядка k

- **Ввод данных:**

- Пользователь указывает количество значений.
- Вводятся пары: значение случайной величины и соответствующая вероятность.

- Вводится порядок момента k .

- Дополнительно предусмотрен режим генерации случайных чисел (при котором вероятности устанавливаются равномерно, то есть $1/N$).

- **Обработка данных:**

- Вычисление момента: сумма произведений каждого значения, возведённого в степень k , на его вероятность.

- **Вывод и запись результата:**

- Вывод результата с форматированием (фиксированная точность) и запись в файл по выбору пользователя.

Модуль 4: Вычисление числа Фибоначчи

- **Ввод данных:**

- Ввод номера числа (от 0 до 93) с клавиатуры или из файла (input4.txt).

- **Обработка данных:**

- Вычисление n-го члена последовательности Фибоначчи.

- **Вывод и запись результата:**

- Результат выводится на экран и может быть записан в файл output.txt.

Модуль 5: Расшифровка сообщения

- **Ввод данных:**

- Ввод справочного текста (количество строк и сами строки) и набора пар индексов (номер строки и номер слова) – с клавиатуры или из файла (input5.txt).

- **Обработка данных:**

- Функция split разделяет строки на слова.
- По каждой паре индексов выбирается слово из справочного текста, формируя итоговое сообщение.

- **Вывод и запись результата:**

- Итоговое (расшифрованное) сообщение выводится на экран и может быть сохранено в файл output.txt.

Модуль 6: Новогодняя открытка (анимация с SFML)

- **Ввод данных:**

- Используются изображения (файлы с картинками Санты, оленя, фона и анимированного текста), которые должны быть доступны в каталоге с программой.

- **Обработка данных:**

- Создаётся окно с помощью SFML.
- Загружаются текстуры и создаются спрайты, затем происходит циклическая смена изображений для создания эффекта анимации.

- **Вывод:**

- Анимация выводится в графическом окне.
- Пользователь может закрыть окно, чтобы завершить модуль.

Модуль 7: Вычисление определителя матрицы 2×2

- **Ввод данных:**

- Ввод элементов матрицы (4 числа) с клавиатуры, из файла (input.txt) или генерация случайными числами.

- **Обработка данных:**

- Вычисление детерминанта по формуле: $\det = a \cdot d - b \cdot c$.

- **Вывод и запись результата:**

- Результат выводится на экран и, по выбору, записывается в файл output.txt.

Завершение работы

- Программа работает циклически – после выполнения выбранного модуля пользователю предлагается вернуться в главное меню или выйти из программы.

4. Состав входных, выходных и промежуточных данных

- **Входные данные:**

- **Модуль 1:** Значения H (максимальная высота) и L (дальность полёта) – положительные числа.

- **Модуль 2:** Число n для вычисления факториала (целое, от 0 до 170).

- **Модуль 3:** Количество значений, пары (x, p) для случайной величины и порядок момента k ; возможно, сгенерированные случайные значения.

- **Модуль 4:** Номер элемента Фибоначчи (целое число от 0 до 93).

- **Модуль 5:** Справочный текст (множество строк) и пары индексов (номер строки, номер слова).

- **Модуль 6:** Изображения для анимации (имена файлов).

- **Модуль 7:** Четыре числа для элементов матрицы 2×2 .

- **Выходные данные:**

- Результаты вычислений (угол и скорость, факториал, момент, число Фибоначчи, расшифрованное сообщение, детерминант).

- Графическая анимация (модуль 6).

- Все результаты дублируются на экране и записываются в файл `output.txt`.

- **Промежуточные данные:**

- Локальные переменные, массивы и структуры (например, для хранения пар (значение, вероятность) или строк справочного текста).

5. Корректные и ошибочные входные данные

- **Корректные данные:**

- Числовые значения, удовлетворяющие условиям задачи (например, положительные H и L ; для факториала – число в диапазоне от 0 до 170; сумма вероятностей равна 1).

- Правильный формат файлов (`input1.txt`, `input2.txt`, `input3.txt`, `input4.txt`, `input5.txt`, `input.txt`).

- **Ошибочные данные:**

- Неположительные числа, ввод букв вместо цифр, недопустимые индексы (в модуле 5) или некорректный формат файлов.

- При вводе вероятностей – если их сумма отличается от 1 (например, меньше 0.99 или больше 1.0).

- Ошибки при открытии файлов (файл не найден или повреждён).

- **Обработка ошибок:**

При обнаружении ошибки программа выводит сообщения вроде:

- «Ошибка! Введите положительное число:»

- «Не удалось открыть файл `inputX.txt` для чтения!»

- «Сумма вероятностей некорректна!»

6. Пользователь и интерфейс

• Пользователь:

Программа ориентирована на студентов, преподавателей и пользователей, выполняющих лабораторные работы по программированию на C++.

• Интерфейс:

- Текстовый консольный интерфейс на русском языке.
- Главное меню с перечислением всех модулей.
- Понятные подсказки при вводе данных, контрольные примеры и сообщения об ошибках.
- Возможность выбора способа ввода данных (с клавиатуры или из файла).

7. Обработка ошибок и сообщения пользователю

• При неверном вводе данных (например, буквы вместо цифр или отрицательные числа) программа очищает поток ввода и выводит сообщение об ошибке с просьбой повторить ввод.

• При отсутствии или ошибках в файлах выводится сообщение о невозможности чтения данных (например, «Не удалось открыть файл inputX.txt для чтения!»).

• Если данные не удовлетворяют требованиям (например, сумма вероятностей не равна 1), выводится сообщение об ошибке, и пользователю предлагается повторить ввод.

8. Ограничения программы

• Диапазоны ввода:

- Для вычисления факториала – число n должно быть в пределах $[0, 170]$.
- Для числа Фибоначчи – n от 0 до 93.

• Зависимость от внешних файлов:

○ Для модулей с вводом из файлов (input1.txt, input2.txt, input3.txt, input4.txt, input5.txt, input.txt) файлы должны существовать и иметь корректный формат.

○ Модуль 6 зависит от наличия изображений (файлы должны быть в рабочем каталоге).

• Защита от некорректного ввода:

- Использование функций проверки ввода (например, функция `durak`).

• Ограничение ресурсов:

○ Программа не предназначена для обработки очень больших объёмов данных, что соответствует требованиям ТЗ.

9. Особые ситуации, требующие специального рассмотрения

• Некорректный формат или отсутствие входного файла:

Программа должна уведомлять пользователя об ошибке и возвращаться в главное меню без аварийного завершения.

- **Некорректный ввод с клавиатуры:**

Использование проверок ввода позволяет избежать сбоев; в случае ошибки выводится соответствующее сообщение, и ввод повторяется.

- **Неверная сумма вероятностей в модуле 3:**

Если сумма введённых вероятностей не равна 1, программа сообщает об ошибке и запрашивает повторный ввод данных.

- **Проблемы с загрузкой изображений (модуль 6):**

Если одно из изображений не загружается, выводится сообщение об ошибке, и модуль завершает работу.

10. Документация

При разработке и сопровождении программы должна быть подготовлена следующая документация:

- **Техническое задание (ТЗ):** Определяет цели, требования и критерии эффективности программы.

- **Спецификация:** Текущий документ, описывающий постановку задачи, анализ, входные/выходные данные, обработку ошибок, ограничения и перспективы развития.

- **Внешняя спецификация:** Описание интерфейса, структуры меню и взаимодействия с пользователем.

- **Документация к исходному коду:** Комментарии в коде, описание функций, структур данных и алгоритмов.

- **Отчёты по лабораторным работам и скриншоты работы программы.**

11. Перспективы развития программы

- **Расширение функционала:**

Добавление новых модулей и задач, расширение возможностей уже существующих (например, более сложные расчёты, работа с большими матрицами, новые алгоритмы).

- **Графический интерфейс:**

Переход от консольного приложения к полноценному GUI с использованием, например, Qt или аналогичных библиотек.

- **Улучшение обработки ошибок:**

Дополнительная валидация входных данных, логирование ошибок и более детальное информирование пользователя.

- **Кроссплатформенность:**

Адаптация программы для работы на других операционных системах (Linux, macOS).

- **Интеграция с другими системами:**

Возможность экспорта/импорта данных в различных форматах (например, CSV, XML), взаимодействие с базами данных.

Данный вариант неверный, так как в момент написания этого запроса у меня отсутствовали полные требования к написанию спецификации. Но после получения учебно-методического пособия «*Методика выполнения лабораторных работ № 1 и № 2 по дисциплине «Технологии и методы программирования»*», в котором были предоставлены точные требования и пример оформления спецификации.

Для следующего запроса я загрузил данное пособие в ChatGPT и написал вот такой запрос: «в данном методическом пособии указано как необходимо оформлять спецификацию. Данная информация указана на 32 странице. Тебе нужно написать спецификацию на основе технического задания и кода программы по примеру, представленному в методическом пособии».

Результат данного запроса (текст слово в слово скопирован из ChatGPT):

Спецификация программы	
Оглавление	
1. Постановка задачи.....	1
1.1. Задача 1: Вычисление начальной скорости и угла броска.....	1
1.2. Задача 2: Вычисление факториала	2
1.3. Задача 3: Вычисление момента порядка k.....	3
1.4. Задача 4: Вычисление числа Фибоначчи.....	4
1.5. Задача 5: Расшифровка сообщения.....	5
1.6. Задача 6: Новогодняя открытка (анимация с SFML).....	6
1.7. Задача 7: Вычисление определителя матрицы 2×2	7
2. Входные и выходные данные для задач.....	8
2.1. Задача 1.....	8
2.2. Задача 2.....	9
2.3. Задача 3.....	10
2.4. Задача 4.....	11
2.5. Задача 5.....	12
2.6. Задача 6.....	13
2.7. Задача 7.....	14
3. Корректные и ошибочные данные.....	15
4. Пользователь программы.....	16
5. Требования к интерфейсу.....	17
6. Необходимая документация.....	18
7. Перспективы развития программы.....	19
1. Постановка задачи	
Разработать единое консольное приложение на языке C++, которое объединяет семь модулей, каждый из которых решает отдельную задачу.	

Программа должна быть защищена от некорректного ввода, обеспечивать циклический режим работы, поддерживать ввод данных как с консоли, так и из файла, а также выводить результаты как на экран, так и в файл.

1.1. Задача 1: Вычисление начальной скорости и угла броска

Описание программы:

Программа принимает значения максимальной высоты подъёма (H) и дальности полёта (L) и, используя физические формулы, вычисляет угол броска и начальную скорость:

- Тангенс угла: $\tan(\alpha) = (4 \cdot H)/L$
- Угол (в радианах) $\alpha = \arctan((4 \cdot H)/L)$, перевод в градусы
- Начальная скорость: $V = \sqrt{(g \cdot L / \sin(2 \cdot \alpha))}$, где $g = 9.81 \text{ м/с}^2$

Шаги реализации:

1. Определение констант (g , π).
2. Ввод данных (H и L) – с консоли или из файла (например, input1.txt), с проверкой корректности ввода.
3. Вычисление тангенса, угла (в радианах и градусах) и начальной скорости.
4. Вывод результатов на экран и запись в файл output.txt.

1.2. Задача 2: Вычисление факториала

Описание программы:

Рассчитывается факториал числа n ($n!$), где n находится в диапазоне $[0, 170]$. Вычисление осуществляется итеративным методом.

Шаги реализации:

1. Ввод числа n (с консоли или из файла input2.txt) с проверкой, что n – целое число в указанном диапазоне.
2. Итеративное вычисление факториала.
3. Вывод результата на экран и запись в файл.

1.3. Задача 3: Вычисление момента порядка k

Описание программы:

По заданному распределению случайной величины (значения x_i и вероятности p_i) и порядку момента k вычисляется момент $M_k = \sum (x_i^k \cdot p_i)$. Возможны варианты ввода: с консоли, из файла (input3.txt) или генерация случайных значений.

Шаги реализации:

1. Ввод количества значений, значений x_i , вероятностей p_i и порядка k с проверкой корректности (например, сумма вероятностей равна 1).
2. Вычисление момента с использованием цикла и формулы.
3. Вывод результата на экран и запись в файл.

1.4. Задача 4: Вычисление числа Фибоначчи

Описание программы:

Программа вычисляет n -й член последовательности Фибоначчи (для n от 0 до 93) по итеративному алгоритму: $F(0)=0$, $F(1)=1$, для $n \geq 2$ $F(n)=F(n-1)+F(n-2)$.

Шаги реализации:

1. Ввод порядкового номера n с проверкой допустимого диапазона ($0 \leq n \leq 93$).

2. Итеративное вычисление члена последовательности.

3. Вывод результата на экран и запись в файл.

1.5. Задача 5: Расшифровка сообщения

Описание программы:

На основании справочного текста (набор строк) и набора пар индексов (номер строки, номер слова) формируется итоговое сообщение. Возможен ввод данных как с консоли, так и из файла (input5.txt).

Шаги реализации:

1. Ввод количества строк и самих строк справочного текста.

2. Ввод количества пар индексов и самих пар.

3. С использованием функции разбиения строки на слова (split) формируется итоговый текст.

4. Вывод расшифрованного сообщения и запись его в файл.

1.6. Задача 6: Новогодняя открытка (анимация с SFML)

Описание программы:

Программа создаёт анимацию новогодней открытки с использованием библиотеки SFML. В анимации участвуют изображения Санты, оленя, фона и анимированного текста, которые циклически меняются.

Шаги реализации:

1. Загрузка необходимых изображений из файлов.

2. Создание окна с помощью SFML и настройка спрайтов (позиции, масштаб).

3. Циклическая смена изображений с задержкой между кадрами.

4. Обработка событий (например, закрытие окна).

5. Вывод графической анимации в окне.

1.7. Задача 7: Вычисление определителя матрицы 2×2

Описание программы:

На основе матрицы 2×2 , элементы которой могут вводиться с клавиатуры, считываться из файла (input.txt) или генерироваться случайно, вычисляется детерминант по формуле: $\det = a \cdot d - b \cdot c$.

Шаги реализации:

1. Ввод или генерация 4 чисел для матрицы с проверкой корректности.
2. Вывод введенной матрицы для контроля.
3. Вычисление детерминанта.
4. Вывод результата на экран и запись в файл.

2. Входные и выходные данные для задач

2.1. Задача 1

– **Входные:**

- N (максимальная высота, положительное число).
- L (дальность полёта, положительное число).
- Переключатель выбора способа ввода (1 – консоль, 2 – файл: input1.txt).

• **Промежуточные:**

- Тангенс угла, угол в радианах и градусах, начальная скорость.

• **Выходные:**

- Вычисленные значения угла и скорости, выводимые на экран и записываемые в output.txt.

2.2. Задача 2

• **Входные:**

- Число n (целое число от 0 до 170), ввод с консоли или из файла input2.txt.

• **Выходные:**

- Факториал числа n , выводимый на экран и в файл.

2.3. Задача 3

• **Входные:**

- Количество значений n (целое число, $0 < n \leq 100$).
- Пары значений: x_i ($0 < x_i \leq 10000$) и p_i ($0 \leq p_i \leq 1$) с проверкой, что сумма p_i равна 1.

- Порядок момента k (целое число, $0 < k \leq 100$).

- Выбор способа ввода (1 – консоль, 2 – файл input3.txt).

• **Выходные:**

- Вычисленный момент M_k , выводимый на экран и записываемый в output.txt.

2.4. Задача 4

• **Входные:**

- Порядковый номер n (целое число от 0 до 93), ввод с консоли или из файла input4.txt.

• **Выходные:**

- n -й член последовательности Фибоначчи, выводимый на экран и записываемый в файл.

2.5. Задача 5

- **Входные:**

- Справочный текст (количество строк и сами строки).
- Пары индексов (номер строки, номер слова) – ввод с консоли или из файла input5.txt.

- **Выходные:**

- Расшифрованное сообщение, выводимое на экран и записываемое в файл.

2.6. Задача 6

- **Входные:**

- Имена файлов с изображениями (санта, олень, фон, анимированный текст).

- Нет дополнительных данных от пользователя.

- **Выходные:**

- Графическая анимация в окне SFML; сообщения об ошибках загрузки при необходимости.

2.7. Задача 7

- **Входные:**

- Четыре числа для элементов матрицы 2×2 – ввод с консоли, из файла (input.txt) или генерация случайных чисел.

- **Выходные:**

- Вычисленный детерминант, выводимый на экран и записываемый в файл.

3. Корректные и ошибочные данные

Общие правила: Для всех задач используется функция проверки ввода (например, CorrectInput). Ниже приведены примеры:

- **Задача 1 (Начальная скорость):**

- Корректные: $N = 5, L = 20$
- Ошибочные: $N \leq 0, L \leq 0, L$ не числовое значение (например, "abc").

- **Задача 2 (Факториал):**

- Корректные: $n = 5, n = 170$
- Ошибочные: $n < 0, n > 170$, некорректный формат ввода (например, "10a").

- **Задача 3 (Момент порядка k):**

- Корректные: $n = 3, k = 4, x = \{1, 3, 5\}, p = \{0.3, 0.2, 0.5\}$
- Ошибочные: $n = 0, n > 100; k \leq 0$ или $k > 100; x[i] \leq 0$ или $x[i] > 10000; p[i] < 0$ или $p[i] > 1$; сумма вероятностей $\neq 1$.

- **Задача 4 (Фибоначчи):**

- Корректные: $0 \leq n \leq 93$
- Ошибочные: $n < 0, n > 93$, нецелое число.

- **Задача 5 (Расшифровка):**

- Корректные: непустой справочный текст, корректные пары индексов, где номера строк и слов соответствуют введённым данным.

- Ошибочные: пустой текст, индексы, выходящие за границы массива слов, неверный формат ввода.

- **Задача 6 (Открытие):**

- Корректные: все изображения доступны в каталоге.

- Ошибочные: отсутствие одного из файлов изображений, что приводит к сообщению об ошибке загрузки.

- **Задача 7 (Определитель):**

- Корректные: 4 числовых значения, удовлетворяющих формату.

- Ошибочные: неверный формат ввода, отсутствие файла, некорректные числа (например, нечисловой ввод).

При возникновении ошибки программа выводит сообщение: «Некорректный ввод. Пожалуйста, попробуйте ввести данные заново.».

4. Пользователь программы

Программа предназначена для студентов, преподавателей и специалистов, участвующих в лабораторных работах по программированию. Пользователь должен обладать базовыми знаниями работы с консольными приложениями и понимать принципы ввода данных.

5. Требования к интерфейсу

- **Язык и оформление:**

Интерфейс программы реализован на русском языке с использованием текстового меню. Для обеспечения удобства работы используется белый шрифт на чёрном фоне.

- **Меню:**

Главное меню должно содержать следующие пункты:

1. Вычисление начальной скорости и угла броска
2. Вычисление факториала
3. Вычисление момента порядка k
4. Вычисление числа Фибоначчи
5. Расшифровка сообщения
6. Новогодняя открытка (анимация)
7. Вычисление определителя матрицы 2×2
8. Выход

При выборе пункта меню выводятся подробные инструкции по вводу данных, сообщения об ошибках и подтверждения записи результатов в файл.

- **Обработка ошибок:**

При неверном вводе пользователь получает сообщение: «Некорректный ввод. Пожалуйста, попробуйте ввести данные заново.».

6. Необходимая документация

В комплект документации должны входить:

- Техническое задание (ТЗ)
- Спецификация (данный документ)
- Внешняя спецификация (при необходимости для подпрограмм, выполняемых разными разработчиками)
- Блок-схемы основного алгоритма и отдельных модулей
- Отчёт о проделанной работе с титульным листом, содержанием, описанием цели работы, примерами входных и выходных данных и скриншотами работы программы.

7. Перспективы развития программы

Программа может быть доработана и расширена в следующих направлениях:

- Добавление новых модулей или задач в соответствии с требованиями заказчика.
- Перенос консольного интерфейса в графический (например, с использованием Qt).
- Реализация экспорта/импорта данных в различных форматах (CSV, XML).
- Улучшение алгоритмов обработки ошибок и добавление системы логирования.
- Модернизация кода для повышения его модифицируемости и адаптации к новым требованиям.

Данная спецификация оформлена в соответствии с методическими рекомендациями (см.) и примером спецификации, приведённым в методическом пособии.

Данный вариант спецификации получился наиболее приближенным к тому, что должно было быть примерно на 80–90 %.

Тем не менее, применение модели сопряжено с рядом ограничений. Во-первых, точность результата зависит от качества и структуры запросов – часто требуется несколько итераций для корректировки формулировок. Во-вторых, модель не всегда учитывает специфические требования образовательного учреждения (госты нумерации, форматирования), что вынуждает вносить ручные правки. Для полного соответствия с требованиями оформления нужно было сделать гиперссылки, исправить рубрикацию и другие недочеты.

Также, был проведен сравнительный тест с альтернативной моделью GigaChat, в результате которого было выявлено, что на данный момент наш отечественный аналог очень сильно уступает ChatGPT. Для честного сравнения, я использовал те же самые запросы, что и для ChatGPT. Модель GigaChat

оказалась менее устойчивой в диалоге, хуже обрабатывала длинные блоки кода, информацию из файлов понимала не полностью и чаще предлагала общие советы вместо точных формулировок.

Результат запросов в GigaChat:

Спецификация программы

Постановка задачи

Программа предназначена для решения семи задач различной тематики: физические расчёты, математические операции и создание анимированной новогодней открытки. Программа должна обеспечить удобную навигацию между модулями, поддерживать ввод данных с клавиатуры и из файлов, а также сохранять результаты вычислений в файл.

Анализ задачи

Программа состоит из семи независимых модулей, каждый из которых реализует отдельную функциональность. Необходимо предусмотреть универсальные механизмы ввода-вывода, контроля корректности данных и сохранения результатов. Интерфейс должен быть интуитивно понятным и лёгким в освоении.

Состав входных, выходных и промежуточных данных

Входные данные

1. Максимальная высота подъёма (H) и дальность полёта (L) – положительные вещественные числа.
2. Число n для вычисления факториала – неотрицательное целое.
3. Количество значений N , случайные величины, их вероятности и порядок момента k – целые и вещественные числа.
4. Порядковый номер числа Фибоначчи – неотрицательное целое.
5. Справочный текст и закодированные пары (номер строки, номер слова) – текстовые данные.
6. Графические ресурсы для новогодней открытки – набор изображений.
7. Элементы матрицы 2×2 – целые числа.

Промежуточные данные

- Результаты расчётов (угол, скорость, факториалы, моменты, числа Фибоначчи, определитель матрицы).
- Индексы строк и слов для декодирования сообщения.
- Текущие кадры анимации.

Выходные данные

- Углы и скорости.
- Факториалы.
- Моменты порядка.

- Числа Фибоначчи.
- Раскодированные сообщения.
- Определитель матрицы.
- Анимированная открытка.

Корректные и ошибочные входные данные

Корректные:

- Положительные вещественные числа для физических расчётов.
- Целые числа в допустимых диапазонах для математических операций.
- Правильно сформированные тексты и индексы для декодирования.

Ошибочные:

- Нулевые или отрицательные значения там, где требуются положительные.
- Числа за пределами допустимого диапазона (например, факториал $n > 170$).
- Некорректные индексы строк и слов.

Пользователи программы

Студенты технических специальностей, преподаватели и специалисты, интересующиеся практическим применением математических и физических моделей.

Интерфейс программы

Консольное меню для выбора модуля. Каждый модуль предлагает опции ввода (с клавиатуры или из файла). Результаты сохраняются в файл output.txt.

Сообщения об ошибках

- «Ошибка! Введите положительное число.».
- «Некорректная пара индексов.».
- «Ошибка чтения файла.».

Ограничения программы

- Максимальный n для факториала ≈ 170 .
- Матрица фиксированного размера 2×2 .
- Анимация зависит от наличия графических ресурсов.

Особые ситуации

- Невозможность открытия файла.
- Превышение допустимых значений.
- Некорректный ввод.

Документация

- Руководство пользователя.
- Описание архитектуры и внутренних механизмов.
- Тестовые сценарии.

Перспективы развития

- Поддержка больших матриц.
- Более сложная графика и анимация.
- Интеграция с веб-интерфейсом.
- Автоматическое тестирование и профилирование.

Результаты данных запросов были даже хуже, чем результат первого запроса в ChatGPT, в котором не было правил оформления спецификации. GigaChat писал информацию из примера в методическом пособии, а не по данным моей программы.

В заключение подчёркиваем, что использование нейросетевых языковых моделей при составлении отчётов и технической документации значительно повышает скорость подготовки материалов и помогает структурировать информацию. Однако результаты генерации требуют внимательной проверки и доработки в соответствии с установленными стандартами. ChatGPT¹⁴ следует рассматривать как вспомогательный инструмент, дополняющий, но не заменяющий аналитические и творческие способности студента.

Васильченко Дарья Алексеевна,

Фролов Максим Андреевич,

*обучающиеся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».*

*Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры
информационной безопасности в управлении Удмуртского
государственного университета,
г. Ижевск*

ИССЛЕДОВАНИЕ УСИЛИТЕЛЕЙ ПЕРЕМЕННОГО НАПРЯЖЕНИЯ, ПОСТРОЕННЫХ НА ОПЕРАЦИОННЫХ УСИЛИТЕЛЯХ

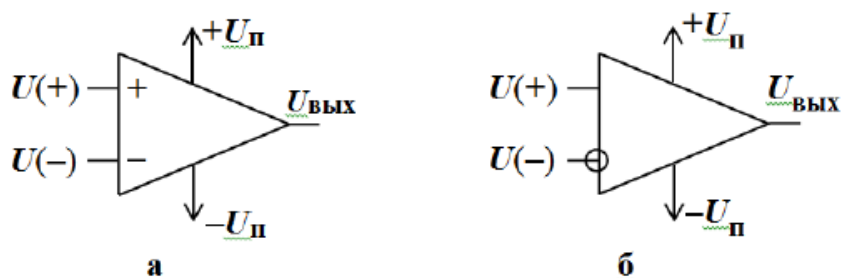
Операционные усилители (ОУ) – интегральные полупроводниковые микросхемы, имеющие несколько усилительных каскадов, причём первый каскад обязательно имеет дифференциальный вход. ОУ первоначально предназна-

¹⁴ OpenAI. ChatGPT: Optimizing Language Models for Dialogue. URL: <https://openai.com/blog/chatgpt> (дата обращения: 15.04.2025).

лись для выполнения различных операций над аналоговыми величинами (отсюда и название) при работе в схеме с отрицательной обратной связью (ООС). В дальнейшем область применения ОУ значительно расширилась – они начали широко применяться в устройствах усиления, генерирования, фильтрации, модулирования и демодулирования сигналов и многих других устройствах.

Несмотря на сложную внутреннюю структуру ОУ может рассматриваться как единый элемент с гарантированными входными и выходными параметрами. Во многих случаях ОУ заменяют идеализированной моделью, имеющей бесконечно большой коэффициент усиления по напряжению K в неограниченной полосе частот D , бесконечно большое входное сопротивление, бесконечно малое выходное сопротивление и бесконечно малое напряжение смещения. Необходимо отметить, что ОУ описываются множеством параметров. Мы коснёмся лишь некоторых основных параметров.

В технической литературе можно встретить различные условные графические обозначения ОУ. Два условных графических обозначения, отличающихся только обозначениями инвертирующего и неинвертирующего входов, приведены на рис. 1.



- (-) – инвертирующий вход ОУ;
- (+) – неинвертирующий вход ОУ;
- $U(-)$ – напряжение на инвертирующем входе;
- $U(+)$ – напряжение на неинвертирующем входе;
- $U_{\text{ВЫХ}}$ – выходное напряжение ОУ;
- $+U_{\text{П}}$ – положительное напряжение питания ОУ;
- $-U_{\text{П}}$ – отрицательное напряжение питания ОУ.

Рис. 1. «Условные графические обозначения ОУ».

Упрощённая схема ОУ представлена на рис. 2. Одной из особенностей структуры ОУ является то, что на входе ОУ установлен дифференциальный каскад. Схема дифференциального каскада представляет собой симметричный мост, содержащий два резистора (R_1 и R_2) и два транзистора (VT_1 и VT_2), в цепь эмиттеров которых включен резистор $R_{э1}$ (рис. 2). Параметры транзисторов VT_1 и VT_2 должны быть одинаковыми, значение сопротивлений резисторов тоже должны быть одинаковыми. В этом случае дифференциальный каскад будет симметричным.

Дифференциальный каскад обладает рядом особенностей:

- малым уровнем дрейфа выходного напряжения каскада (выходным напряжением дифференциального каскада является напряжение между коллекторами транзисторов VT1 и VT2) из-за колебаний температуры, напряжений источников питания и старения элементов;
- высоким коэффициентом усиления дифференциального входного напряжения (т.е. разности напряжений входных сигналов);
- низким коэффициентом усиления по отношению к синфазным входным сигналам, следовательно, высоким подавлением синфазных помех на входе дифференциального каскада;
- высоким входным сопротивлением по отношению к поданным на его входы сигналам (дифференциальным и синфазным сигналам);
- требует наличия двухполярного источника питания.

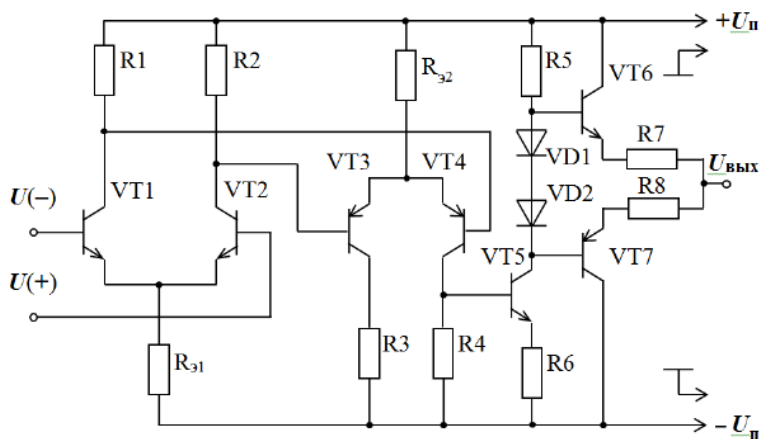


Рис. 2. «Упрощённая схема ОУ».

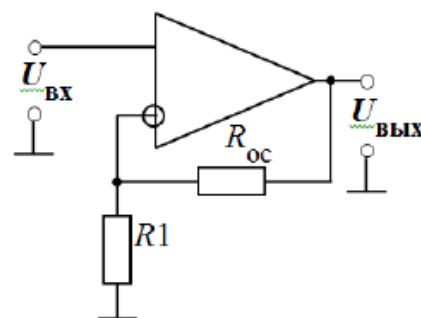


Рис. 3. Схема неинвертирующего усилителя напряжения на ОУ.

ОУ имеет в своём составе второй дифференциальный каскад на транзисторах VT3 и VT4 (рис. 2), но с несимметричным выходом, так как именно такой выход требуется для подачи сигнала на усилительный каскад на транзисторе VT5, включенном по схеме с общим эмиттером. На транзисторах VT6 и VT7 выполнен выходной (оконечный) каскад. Он работает в режиме АВ. Начальное смещение для выходного каскада получают с помощью диодов VD1 и VD2. Резисторы R7 и R8 являются токоограничивающими: при подключении к выходу ОУ низкоомной нагрузки или короткого замыкания выхода ОУ эти резисторы ограничивают максимальное значение выходного тока, предотвращая выход из строя выходных транзисторов VT6 и VT7.

Обычно ОУ имеют маломощные выходные каскады, не рассчитанные на достаточно большие токи (сотни миллиампер и амперы), поэтому в УЗЧ на ОУ обычно строят входные каскады и каскады предварительного усиления.

Известно три основных схемы включения ОУ в качестве усилителя напряжения: схема неинвертирующего усилителя, схема повторителя напряжения и схема инвертирующего усилителя (рис. 3).

Неинвертирующий усилитель (рис. 3) усиливает входной сигнал $U_{вх}$, оставляя неизменной его фазу на выходе по отношению к фазе сигнала на входе. Коэффициент усиления по напряжению неинвертирующего усилителя равен

$$K_U = \frac{R_{oc}}{R_1} + 1 \quad (1)$$

Резистор R_{oc} – это резистор обратной связи, участвующий в подаче части сигнала с выхода ОУ на его инвертирующий вход.

В качестве экспериментальной части мы составили задания, к которым описали шаги для их выполнения¹⁵.

Определить с помощью осциллографа коэффициент усиления неинвертирующего усилителя при значениях $R_1 = 10\text{кОм}$, $R_{oc} = 20\text{кОм}$ и сопротивлении нагрузки 2кОм на частоте 1кГц . Снять осциллограммы входного и выходного сигналов.

Пояснения к выполнению. В Micro-Cap соберите схему неинвертирующего усилителя на ОУ, представленную на рис. 4.

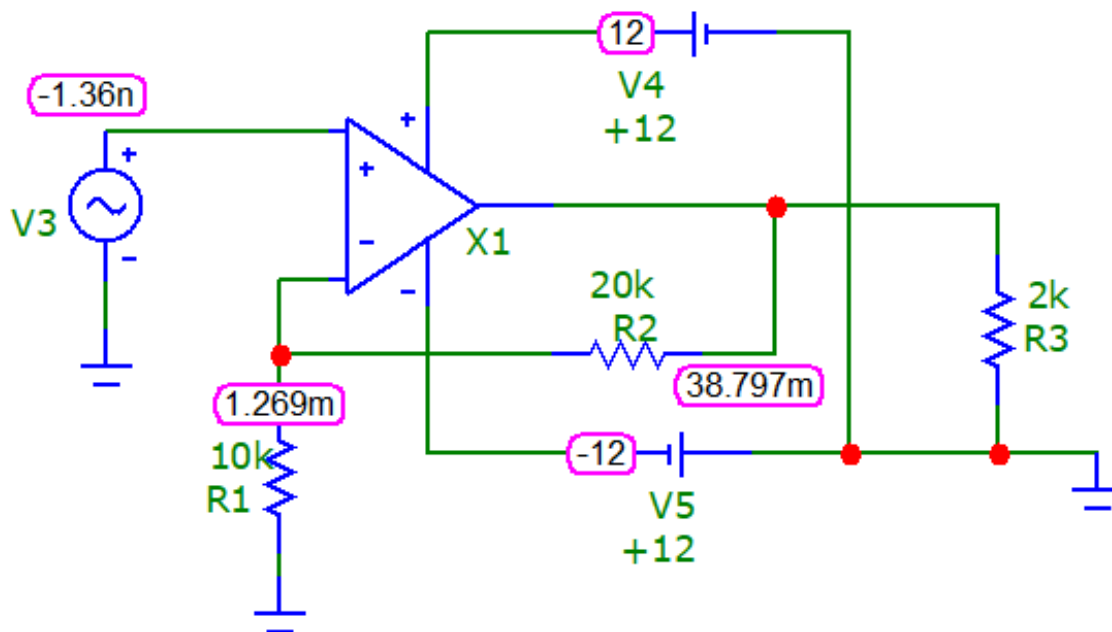


Рис. 4. Схема для исследования неинвертирующего усилителя.

Установите на источнике синусоидальных сигналов, подключенном ко входу усилительного каскада, частоту синусоидального колебания 1кГц и амплитуду 1В . (см. рис. 5 на стр. 40).

¹⁵ Медведев И.И. Схемотехника аналоговых электронных устройств : лабораторный практикум. Брянск : БГТУ, 2020. 64 с.

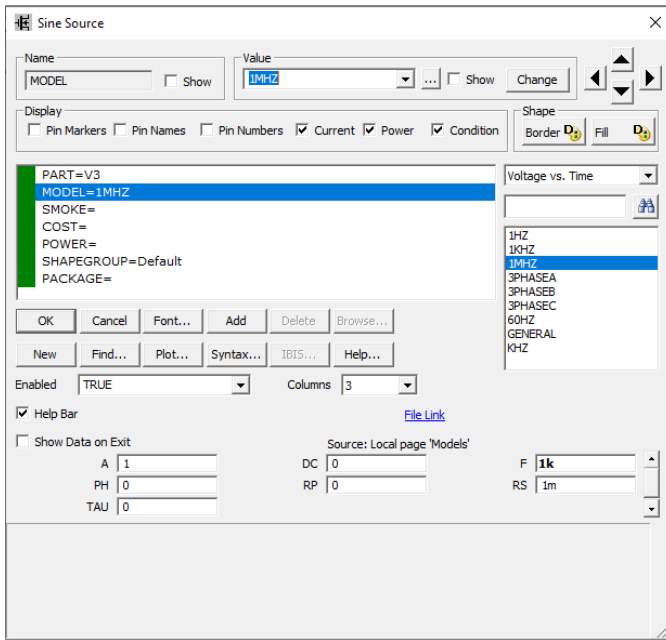


Рис. 5. Значения для источника синусоидальных сигналов.

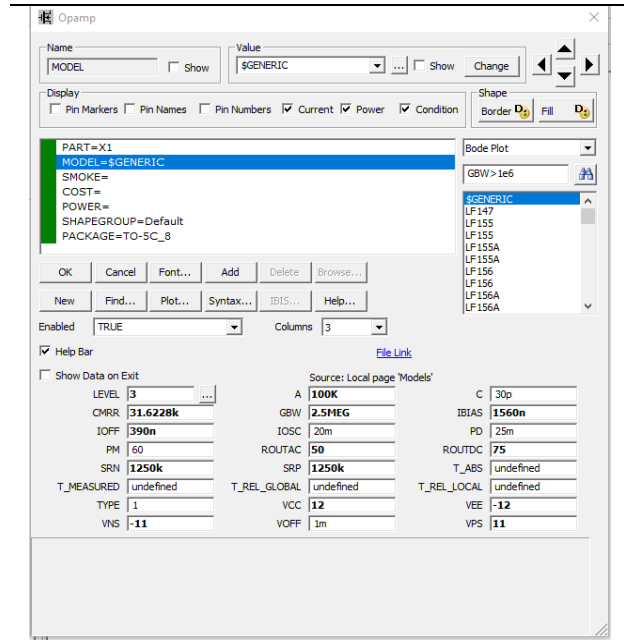


Рис. 6. Значения для ОУ.

Установите на ОУ значения согласно рис. 6.

Для того чтобы использовать осциллограф в Micro-Cap необходимо найти на панели инструментов «Analysis» -> «Transient». В открывшемся окне необходимо использовать следующие значения (рис. 7) и нажать кнопку «Run».

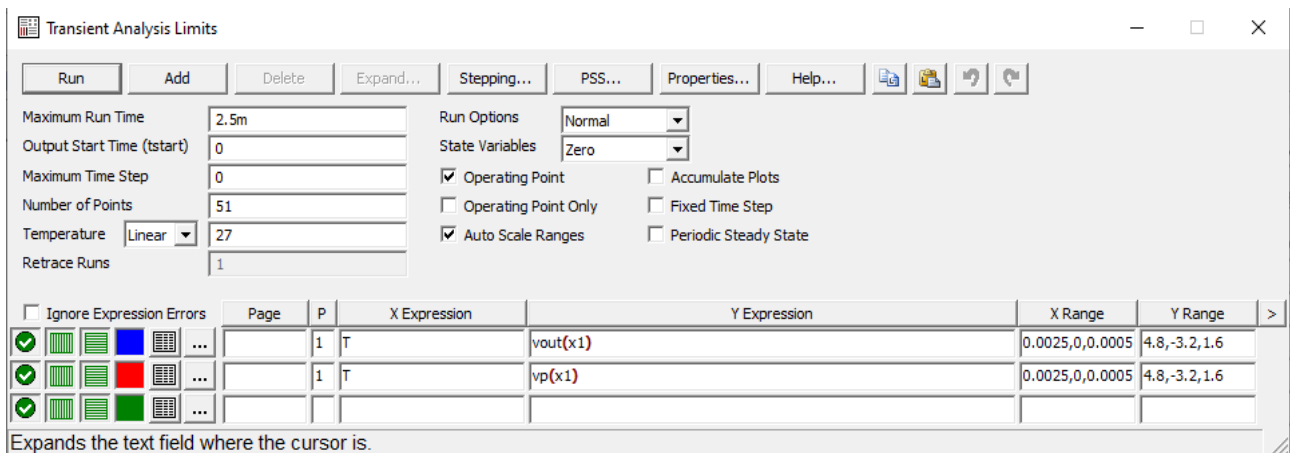


Рис. 7. Осциллограммы Входного и Выходного сигналов.

Рассчитайте коэффициент усиления неинвертирующего усилителя по напряжению

$$K_U = \frac{U_{M \text{ Вых}}}{U_{M \text{ Вх}}} \quad (3)$$

Рассчитайте коэффициент усиления неинвертирующего усилителя по напряжению K_U по формуле (4). Учтите, что $R_{oc} = R_2$.

$$K_U = \frac{R_2}{R_1} + 1 \quad (4)$$

Сравните результаты расчётов коэффициентов усиления неинвертирующего усилителя по напряжению K_U .

Снять амплитудно-частотную характеристику (АЧХ) неинвертирующего усилителя.

Пояснение к выполнению. Чтобы снять АЧХ для схемы, изображенной на рисунке 1 необходимо на панели инструментов открыть «Analysis» – «AC». Для снятия АЧХ проставьте значения как на рисунке 8.

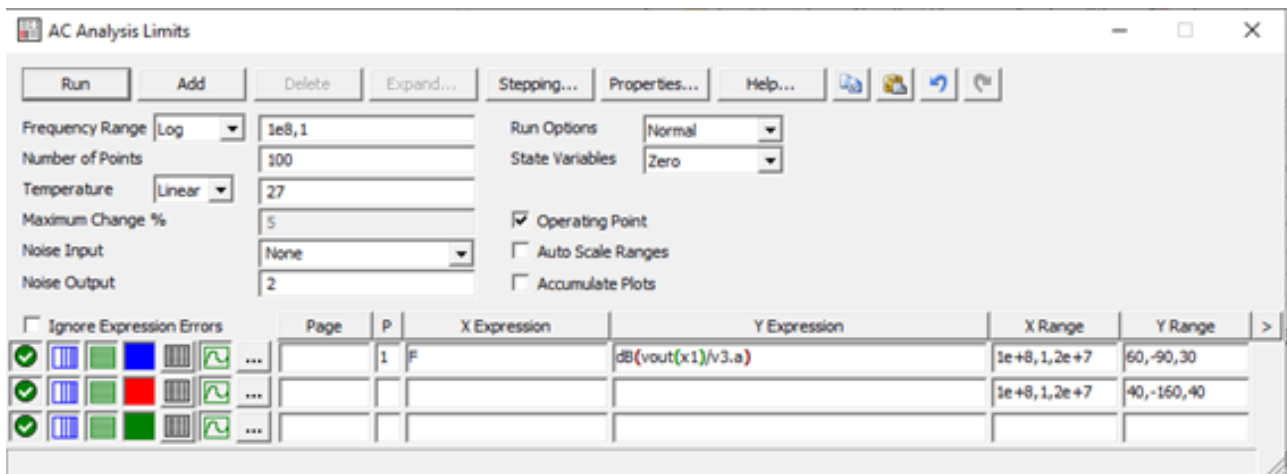


Рис. 8. Снятие АЧХ неинвертирующего усилителя.

Полученную АЧХ приведите в отчёте о лабораторной работе и укажите граничные частоты АЧХ по уровню 0.707, а также коэффициент усилителя на частоте 1кГц.

Сравните значения коэффициентов усиления по напряжению, полученные в текущем и предыдущем заданиях.

Пример выполнения данной работы

1. Собрали схему и выставили значения из условия задания для источника, ОУ и других элементов.

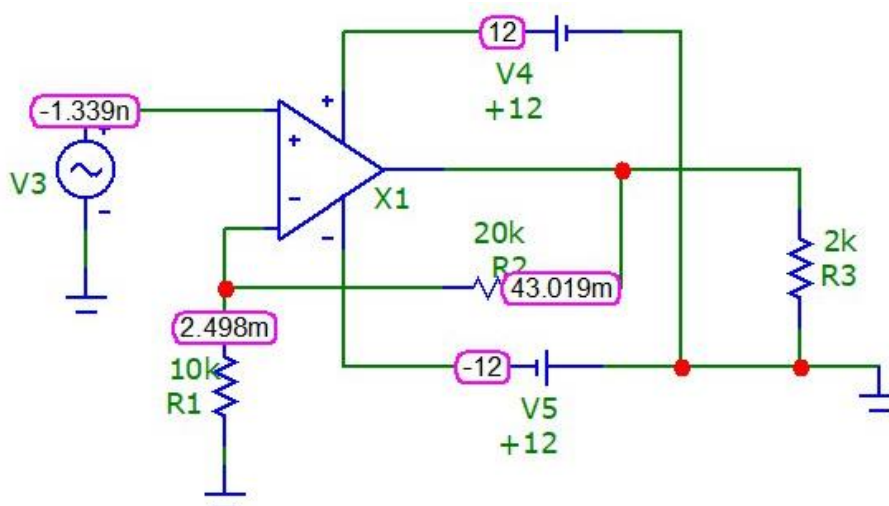


Рис. 9. Схема неинвертирующего усилителя.

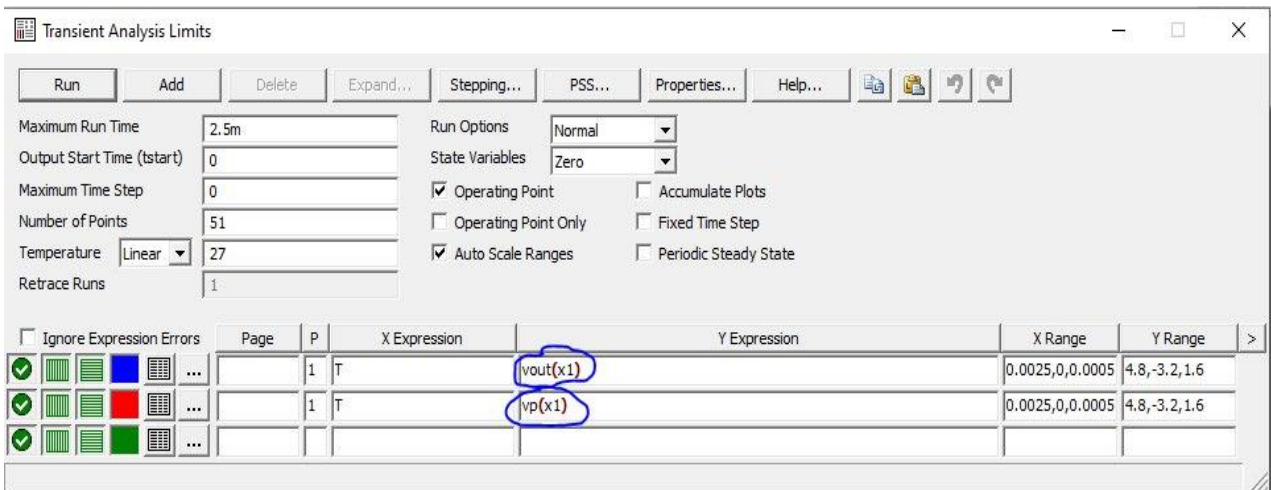


Рис. 10. Снятие осциллограммы входного и выходного сигналов.

2. Открыли analysis -> transient и вписали параметры как на рисунке 10, т.е. выход ОУ и положительный вход ОУ.

3. Нажали Run и получили: красное – входной сигнал, синее – выходной.

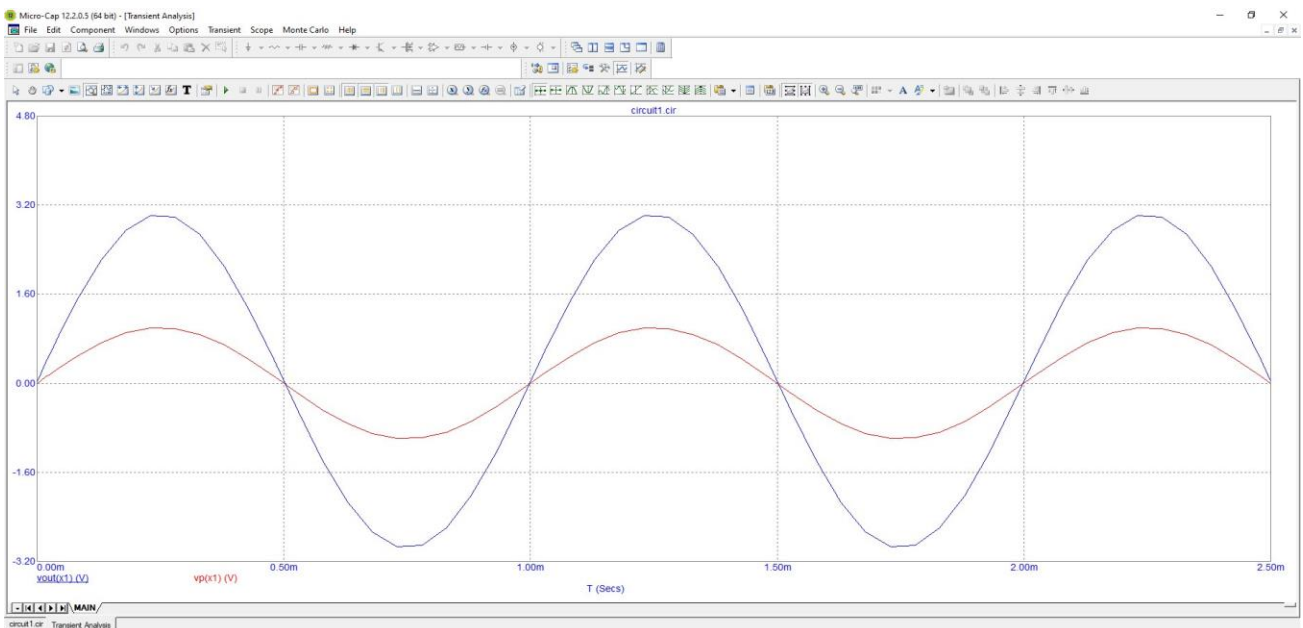


Рис. 11. Осциллограммы входного (красный) и выходного (синий) сигналов.

4. С помощью курсора посмотрели значения в вершинах сигнала и узнали, что у красного 1 В, а у синего – 3 В. Делим Выходной сигнал на входной $3/1$ получаем 3 – это коэффициент усиления, проверить можно формулой $(R2/R1) + 1$. В нашем случае $R2 = R_{oc} \Rightarrow (20/10) + 1 = 3$, что соответствует экспериментальным вычислениям.

1. Чтобы изучить АЧХ мы использовали Analysis -> AC и в открывшемся окне вставили значения как на рисунке 12 и нажали Run.

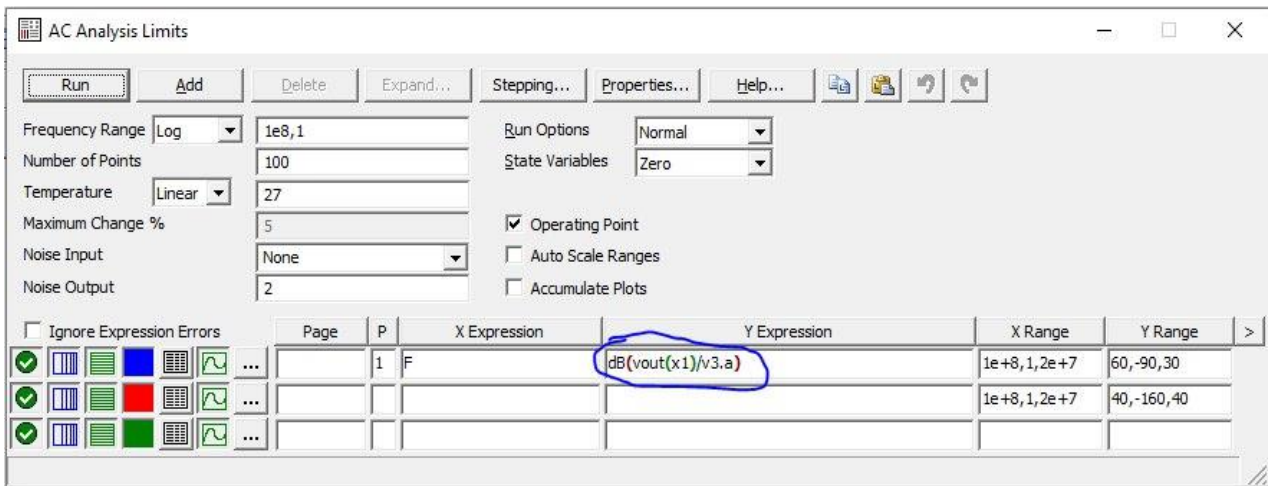


Рис. 12. Снятие АЧХ неинвертирующего усилителя.

Мы получили график изображенный на рисунке 13, стрелками показаны основные моменты: самая левая показывает усиление в децибелах и равно 9.54. Мы знаем, что у нас ОУ работает на частоте 2.5 МГц => основное падение усиления начнётся на $2.5/3 = 833,33$ кГц что соответствует падению на 3дБ. Между 2 стрелками справа можно найти точку 833 кГц и усиление в этой точке примерно равно 6.54, что соответствует теоретической.

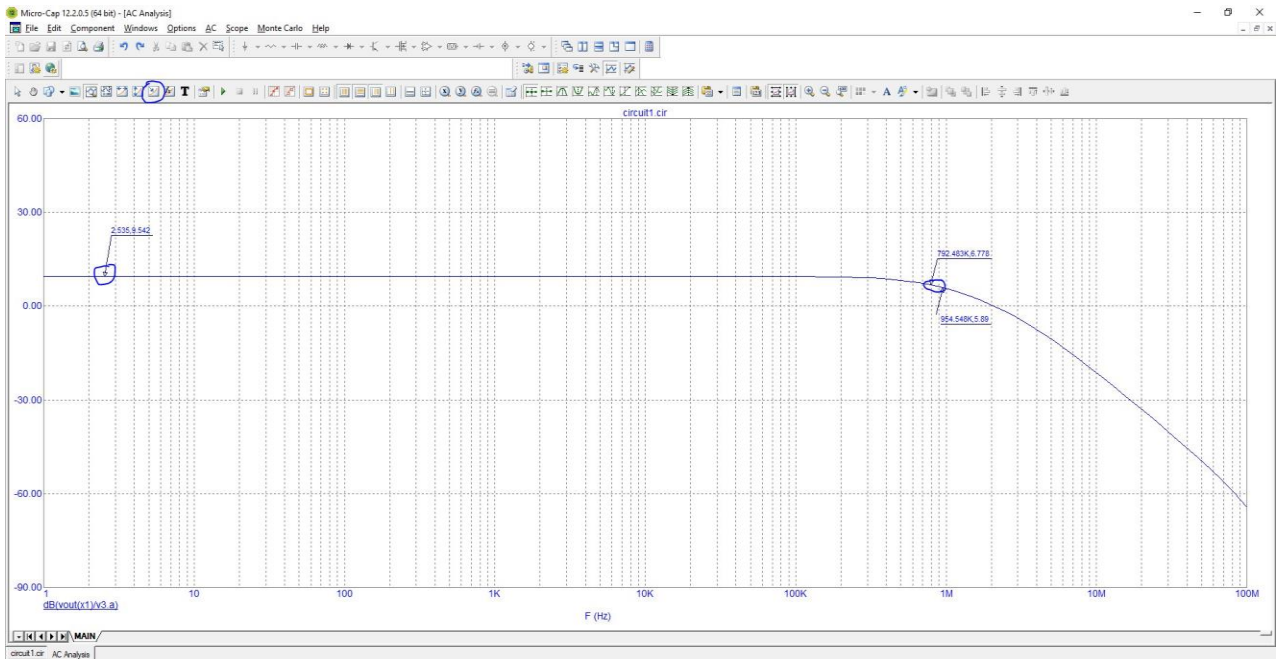


Рис. 13. График АЧХ неинвертирующего усилителя.

Власенко Иван Петрович,

обучающийся 5 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры

информационной безопасности в управлении Удмуртского

государственного университета,

г. Ижевск

СПОСОБЫ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ЦЕПЯМ ЭЛЕКТРОПИТАНИЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

В современном цифровом мире информация является одним из самых ценных активов и её защита от несанкционированного доступа – это необходимость, диктуемая законодательством. Одним из основных направлений защиты информации является защита от технических каналов утечки информации. К ним относят следующие каналы: визуально-оптические каналы, акустические, радиоэлектронные и материально-вещественные.

Каждый из этих видов по-своему опасен:

– визуально-оптический канал связаны с дистанционным считыванием данных и ее фиксацией с носителей информации. В качестве примера через данный канал можно реализовать следующие угрозы: фотографирование документов, экранов мониторов с конфиденциальной информацией, ведение видеосъемки тех же объектов¹⁶;

– радиоэлектронный канал утечки информации реализуется через передачу информации с помощью электрического тока и электромагнитных волн, так как они являются носителями информации. Передача осуществляется через среду (воздушное и безвоздушное пространство) с использованием опасных сигналов или закладных устройств¹⁷;

– акустический канал утечки информации для передачи информации использует акустические волны, которые распространяются в газовой среде.

¹⁶ Визуально-оптический канал утечки информации // Бюллетень научно-технической информации : [сайт]. URL: <http://www.bnti.ru/showart.asp?aid=45&lvl=04.02.04.&p=1> (дата обращения: 15.05.2024).

¹⁷ Радиоэлектронные каналы утечки информации и средства перехвата радиосигналов // Spravochnik.ru : [сайт]. URL: https://spravochnik.ru/informatika/radioelektronnye_kanalny_utechki_informacii_i_sredstva_perehvata_radiosignalov/ (дата обращения: 15.05.2024).

Для реализации данного канала используются направленные микрофоны, диктофоны, а также специальные закладочные устройства¹⁸;

– материально-вещественный канал утечки – это получение информации путем кражи физического носителя или копирования данных с него. Среди угроз осуществимых через данный канал относят кражу документов, флэш носителей, жестких дисков и т.д.¹⁹.

Одним из самых опасных из них является радиоэлектронный канал, так как он самый тяжелый с точки зрения защиты. Обнаружение утечки через подобный канал сложно заметить, радиоэлектронные сигналы, а также электромагнитные излучения от электронных устройств, проникают повсюду. Полностью изолировать от них пространство практически невозможно. А перехват информации через данный канал может производиться на большом расстоянии и в больших объемах.

Данный вид канала делится еще на три подвида:

– электромагнитные – информация передается с помощью электромагнитных волн, распространяющихся в воздушной и безвоздушной среде;

– электрические – информация передается в виде электрического тока по электрическим цепям;

– индукционные – информация передается посредством электромагнитной индукцией, когда изменение тока в одном проводнике создает электродвижущую силу (ЭДС) в другом, близко расположенном проводнике.

Предлагаю подробнее рассмотреть защиту от данных каналов утечки информации по цепям электропитания.

Самая распространённая система электропитания зданий состоит из трансформаторной подстанции и трёхфазной линии передач, в которой имеются три фазных проводника L1, L2, L3, а также совмещённые защитный нейтральный и защитный заземляющий проводник PEN (см. рис. 1 на стр. 46).

¹⁸ Хорев А.А. Технические каналы утечки акустической (речевой) информации // Бюллетень научно-технической информации : [сайт]. URL: <http://www.bnti.ru/showart.asp?aid=957&lvl=04.02> (дата обращения: 15.05.2024).

¹⁹ Основные каналы утечки информации // RT-Solar : [сайт]. URL: https://rt-solar.ru/products/solar_dozor/blog/2085/ (дата обращения: 15.05.2024).

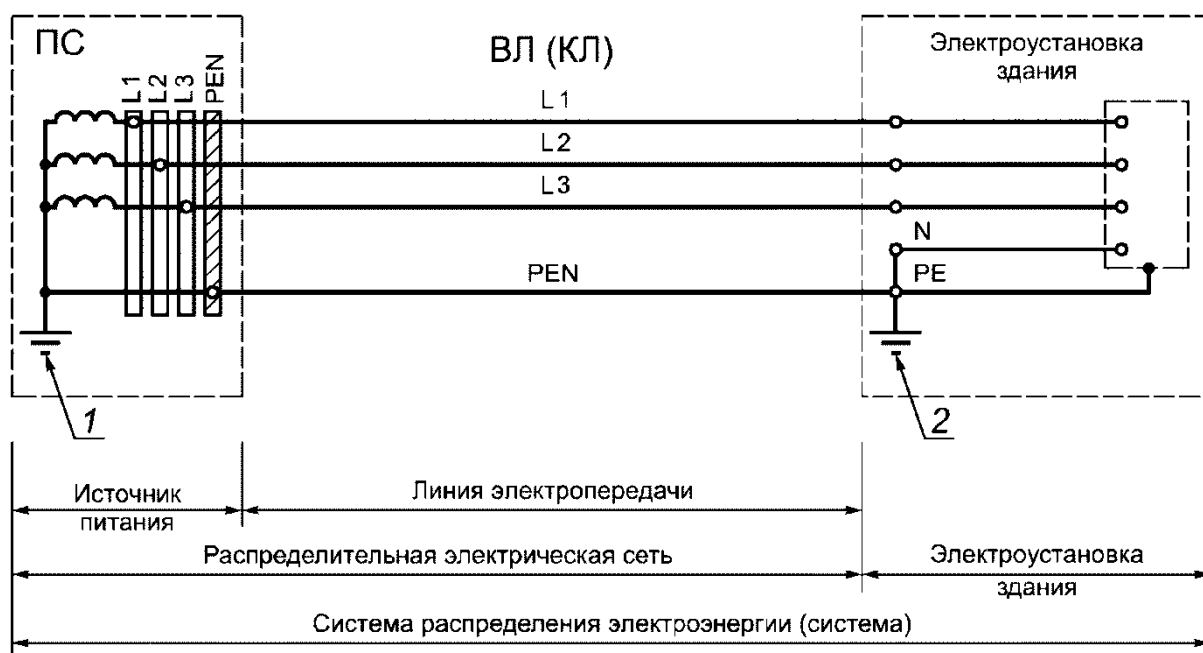


Рис. 1 Общий вид системы электропитания здания: 1, 2 – заземляющие устройства.

Существует две основные угрозы, связанные с утечкой информации по цепям электропитания, от которых необходимо обеспечить защиту:

- наводки побочных электромагнитных излучений технических средств хранения и обработки информации, а также линии их передачи;
- установка закладных устройств в сети электропитания для передачи информации за пределы контролируемой зоны.

Наводки побочных электромагнитных излучений (ПЭМИ) представляют собой нежелательные электромагнитные сигналы, возникающие в результате работы электронных устройств и распространяющиеся по различным путям, включая пространство и линии связи. ПЭМИ содержат информацию о конфиденциальных данных (паролях, коммерческой тайне, личной переписке и т.д.), обрабатываемых или хранящихся в средствах вычислительной техники. Злоумышленники могут использовать специализированное оборудование для перехвата электромагнитных излучений, извлекая конфиденциальную информацию без прямого доступа.

Закладное устройство – это электронное устройство, созданное для несанкционированного съема информации. Данные устройства скрытно размещаются злоумышленниками в организации. Устройство представляет собой ретранслятор, на его вход поступает первичный сигнал, содержащий полезную информацию, а на выходе сигнала распространяется через среду. По виду носителя информации закладные устройства делятся на проводные и излучающие. Проводные передают данные по электрическим проводам, а излучающие с по-

мощью радиосигналов²⁰. Типовая структурная схема закладного устройства представлена на рис. 2. Под следующими цифрами обозначается следующее: 1 – микрофон; 2 – усилитель звукового диапазона; 3 – генератор высокой частоты; 4 – модулятор; 5 – высоко-частотный усилитель; 6 – фильтр для согласования с сетью 220 В; 7 – вторичный источник питания.

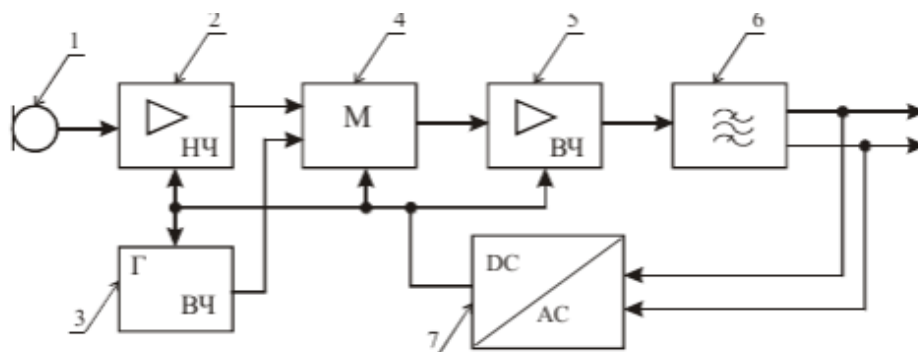


Рис. 2. Типовая структурная схема закладного устройства.

Для защиты от данных угроз применяются следующие принципы и подходы²¹:

- организационные-технические мероприятия;
- пассивные методы защиты;
- активные методы защиты;
- выявление закладочных устройств;
- комплексный подход.

Организационно-технические мероприятия – это совокупность действий, направленных на применение организационных и технических мер защиты информации на объекте информатизации. К таким мерам можно отнести выполнение следующих требований²²:

- организация контролируемой зоны, а именно создание территория или пространство, на которых исключено неконтролируемое пребывание лиц или транспортных средств без постоянного или разового допуска;
- осуществление электропитания от трансформаторной подстанции, расположенной в контролируемой зоне;

²⁰ Хорев А.А. Классификация электронных устройств перехвата информации // Бюллетень научно-технической информации : [сайт]. URL: <http://www.bnti.ru/showart.asp?aid=907&lvl=04.01> (дата обращения: 15.05.2024).

²¹ Трушин В.А., Быков С.В. Защита конфиденциальной информации от утечки по цепям электропитания : учебно-метод. пособие. Новосибирск : НГТУ, 2007. 36 с.

²² Хорев А.А. Способы защиты объектов информатизации от утечки информации по техническим каналам: защита цепей электропитания средств вычислительной техники // Бюллетень научно-технической информации : [сайт]. URL: <http://www.bnti.ru/showart.asp?aid=1016&lvl=04.02> (дата обращения: 15.05.2024).

– помещения с распределительными устройствами и силовыми щитами должны закрываться на замок и опечатываться;

– установка подключения питания средств вычислительной техники, рекомендуется выполнять от одной фазы или от отдельного щитка;

– заземляющие устройства объекта информатизации и трансформаторной подстанции должны находиться в пределах контролируемой зоны.

Пассивными методами защиты направлены на уменьшение уровня сигнала в месте возможного ее перехвата. Это осуществляется с помощью экранирования линий электропередач, установка помехоподавляющих фильтров, разнесением кабелей, а также использование разделительных трансформаторов. Но большое внимание уделяется именно фильтрации опасных сигналов с помощью фильтров.

Основное назначение фильтров - это пропуск сигналов, находящихся в рабочей полосе частот, и подавления сигналов за пределами данной полосы частот. На данный момент существует большое количество видов помехоподавляющих фильтров. Выделяют три основных вида:

- фильтры низких частот (LC-фильтры) – работают на частоте до 300 МГц;
- коаксиальные, полосовые и волноводные – работают на частотах выше 1 ГГц;
- комбинированные – работают в диапазоне частот от 300 МГц до 1 ГГц.

В качестве примера можно привести такие типы фильтров как ФП, ФСПК, ФСП, ЛФС. Принципиальная схема ФП-12...14 представлена на рис. 3.

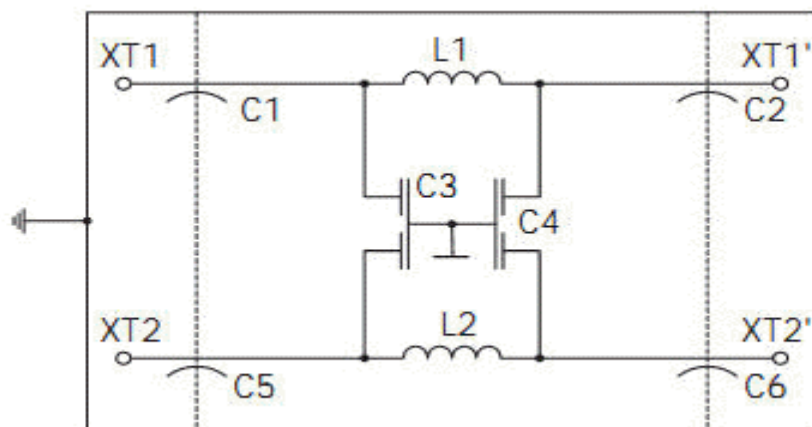


Рис. 3. Принципиальная схема помехоподавляющего фильтра, обеспечивающего эффективность фильтрации опасных сигналов не менее 80 дБ.

К активным способам защиты относят маскирование информативных сигналов специально созданными шумовыми сигналами. Осуществляется это с помощью применения систем линейного зашумления. Подобные системы также называются генераторами шума. Они подключаются к линии электропередач и увеличивают уровень шума, который подается на закладное устрой-

ство, тем самым ухудшая качества сигнала и уменьшая возможность его компрометации. В качестве примера можно назвать следующие модели генераторов шума: SEL SP-44, ЛГШ-221, Соната-РС1, Соната-РС2 и т.д.

Типовая структурная схема генератора линейного зашумления представлена на рис. 4. Цифрами обозначаются: 1 – задающий генератор шума; 2 – широкополосный усилитель; 3 – фильтр для согласования с сетью 220 В; 4 – вторичный источник питания.

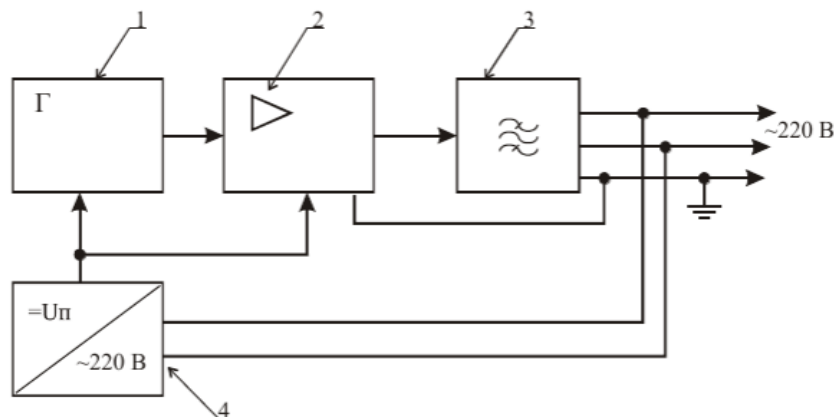


Рис. 4. Типовая структурная схема генератора линейного зашумления.

Метод выявления закладочных устройств направлен на нахождение закладочных устройств в цепи электропитания. Для этого используются специальные приборы. Среди таких можно назвать нелинейные локаторы, индикаторы поля, сканирующие приемники, анализаторы спектра, а также программно-аппаратные комплексы.

Нелинейные локаторы обнаруживают закладные устройства по содержащимся в них полупроводниковым компонентам, таким как диоды, транзисторы и микросхемы. Принцип действия основан на облучении окружающего пространства, а полупроводниковые приборы находящиеся в помещении переизлучают сигнал, который затем регистрируется нелинейным локатором²³.

Индикаторы поля позволяют обнаружить малогабаритные закладные устройства. Индикаторы улавливают радиоизлучения в диапазоне от 30 МГц до 10 ГГц. Работают на расстоянии одного метра, при обнаружении закладного устройства срабатывает звуковая и световая сигнализация²⁴.

Сканирующие приемники так же, как и индикаторы поля, позволяют обнаружить радиозакладки, но в отличие от них имеет более широкий частотный диапазон, способны работать со всеми видами модуляции и позволяют произвести точную настройку.

²³ Нелинейный локатор: что это и для чего он нужен? // Поиск Жучков : [сайт]. URL: <https://поиск-жучков.рф/blog/nelinejnyj-lokator-chto-eto-i-dlya-chego-on-nuzhen/> (дата обращения: 15.05.2024).

²⁴ Индикатор электромагнитного поля // Поиск Жучков : [сайт]. URL: <https://поиск-жучков.рф/blog/indikator-elektromagnitnogo-polya/> (дата обращения: 15.05.2024).

Комплексный подход совмещает в себе комбинации способов, а именно одновременное использование организационных методов, активного и пассивного подходов, а также поиск закладных устройств. Этот вариант применяется в большинстве организаций, так как совмещение подходов обеспечивает более надежную защиту, а также это позволяет избавиться от угроз, появляющихся при невозможности исполнения полных мер защита для одного из подходов.

Таким образом, были рассмотрены основные способы защиты информации от утечки по цепям электропитания.

Гарафиева Венера Равилевна,

обучающаяся 4 курса Информационной безопасности ИФ УУНУТ.

Научный руководитель: А.Р. Аюпова, к.ф.-м.н., доцент кафедры

математического моделирования и информационной безопасности

Нефтекамского филиала Уфимского университета науки и технологий,

г. Нефтекамск

ВНЕДРЕНИЕ КОНЦЕПЦИИ BYOD В ПОЛИТИКУ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Концепция Bring Your own Device берет свое начало с нулевых, когда работники стали предпочитать собственные мобильные устройства корпоративным, выдаваемых в то время. Увеличивался рост числа удаленных и гибридных рабочих мест в организациях, а также открытие корпоративных сетей для поставщиков и подрядчиков, вынудили расширить политику BYOD и учесть в ней персональные компьютеры, ноутбуки, планшеты и др. Такие события как пандемия и последовавший за ней дефицит чипов привели к тому что большая часть организаций была вынуждена принять политику «принести свое собственное устройство» и дать возможность сотрудникам работать с собственных устройств, до тех пор, пока те не получают устройства от компании.

Bring your own device (BYOD) – корпоративная политика для IT-компаний, которая поощряет использование персональных устройств пользователя для выполнения рабочих задач.

По данным Глобальной Отраслевой Аналитики, начиная с 2024 года объем мирового рынка средств обеспечения безопасности BYOD составил 46 миллиардов долларов США. Аналитики предсказывают, что данный показатель сможет вырасти до 133 миллиардов долларов США, со стабильным среднегодовым ростом в 19,4 %. Сегмент затрагивающий безопасность смартфонов, достигнет

отметки среднегодового роста в 20,9 %, и к концу анализируемого периода составит 81,7 миллиарда долларов США. Среднегодовой темп роста сегмента безопасности ноутбуков оценивается в 17,4 % в годовом исчислении, все за тот же анализируемый период²⁵.

Развитие концепции BYOD принесло с собой не только гибкость и экономии средств для компаний, но и соответствующие трудности, связанные с безопасностью персонального устройства. Одной из главных проблем присущих организациям, это отсутствие прямого контроля отдела информационных технологий над персональными устройствами сотрудника. Конечно в таком случае, необходимо учитывать различие по аппаратному и программному обеспечению, а также настройкам безопасности. Персональные устройства зачастую не соответствуют корпоративным политикам безопасности, а организациям в свою очередь трудно обеспечить необходимое соблюдение данных политик на персональных устройствах сотрудников. Равным образом это открывает брешь для множества уязвимостей, включая риск заражения программного обеспечения, возможного несанкционированного доступа к корпоративным сетям и конфиденциальным данным, а также утечек данных.

Учитывая удаленную работу сотрудника, необходимо брать во внимание и человеческий фактор, который может повлечь за собой нарушение безопасности. Многие пользователи зачастую не обновляют свою операционную систему, что влияет на работу отдельного ПО, так же могут не иметь надежной антивирусной программы, или пароля, соответствующего требованиям парольной аутентификации. Все перечисленные факторы, делают пользователя легкой мишенью для киберпреступников.

При работе с персональными устройствами важно учитывать и сеть, к которой подключается работник, учитывая нынешнюю тенденцию сотрудников работать ото всюду, включая общедоступные незащищенные сети в общественных местах, таких как аэропорты, кафе и коворкинги. В таких местах велик шанс стать жертвой атаки «человек посередине», что в свою очередь повлечет вмешательство в протокол передачи информации, способствуя удалению или искажению информации. Подобные угрозы способствуют усилению политики безопасности компаний в области защиты информации, которая в последствии приведет к пересмотру построения архитектуры безопасности, для возможности защиты конфиденциальной информации, даже с учетом использования разных видов персональных устройств и локаций с которых те были подключены к корпоративной сети.

²⁵ *BYOD Security* // Market Research.com. 2025. URL: <https://www.marketresearch.com/Global-Industry-Analysts-v1039/BYOD-Security-39501375/> (дата обращения: 11.04.2025).

Вопросы юридического характера, а также вопросы соответствия требованиям имеют не меньший вес в безопасности BYOD. По мере ужесточения правил защиты данных, таких как General Data Protection Regulation (GDPR) и Health Insurance Portability and Accountability Act (HIPAA), отечественными аналогами данных законов будут выступать Федеральный закон «О персональных данных» от 27.07.2006²⁶, а также приказы ФСТЭК, организации должны обеспечить доступ личных устройств к корпоративным данным, соответствуя тем же стандартам безопасности и соответствия, что и устройства, принадлежащие компании. Организации обязаны предоставить гарантию того, что персональные устройства, используемые сотрудниками, будут соответствовать тем же требованиям безопасности, что и оборудование, предоставляемое компанией. В случае если произойдет компрометация персонального устройства сотрудника, необходимо установить границы, в которых ответственность за утечку данных будет нести либо компания, либо сам сотрудник. Руководству компании придется решить и такой вопрос как обезопасить предприятие в случае увольнения сотрудника, поскольку в этом случае будет необходимостью проконтролировать имеющуюся информацию на персональном устройстве сотрудника. Основой для решения данной задачи будет создание четко структурированной политики BYOD, в которой ясно будут прописаны обязанности и границы ответственности обеих сторон. Подобная политика должна находить баланс между защитой конфиденциальной информацией компании, соблюдением федеральных законов и снижением рисков для бизнеса²⁷.

В состав BYOD входит два компонента: инфраструктура рабочих столов (VDI), а также управление мобильными устройствами (MAM). Однако прежде чем внедрить подобные решения, необходимо провести инвентаризацию мобильных устройств и IT-инфраструктуры, чтобы понять текущие потребности и рабочие нагрузки. На этапе рационализации определяется стандартное ПО для мобильных устройств и формируются требования для подготовки инсталляционных пакетов²⁸. Компании всё чаще внедряют архитектуру Zero Trust, основанную на принципе, согласно которому любое устройство или пользователь, независимо от их местоположения, потенциально могут представлять угрозу. Это требует постоянной проверки подлинности и авторизации перед предоставлением доступа к корпоративным ресурсам. Кроме того, активно применяются технологии искусственного интеллекта и машинного обучения в системах

²⁶ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ // Consultant.ru : [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 12.04.2025).

²⁷ Дорощев А.В., Марков А.С. Методические основы киберучений и CTF-соревнований М., 2022. С. 56-63 (дата обращения: 12.04.2025).

²⁸ Как спроектировать рабочее место. BYOD // habr.com. : [сайт]. 2025. URL: https://habr.com/ru/companies/icl_group/articles/273707/ (дата обращения: 12.04.2025).

кибербезопасности. Это позволяет в режиме реального времени выявлять и устранять угрозы, включая подозрительное поведение устройств. Стандартными рекомендациями по оборудованию рабочего места будут:

- облачные сервисы;
- MDM решение для управления политиками на устройствах;
- портал корпоративных приложений, интегрированный с системой управления корпоративной средой;
- виртуальные рабочие столы;
- виртуализация пользовательского окружения.

Устаревание операционных систем, слабые пароли и небезопасные Wi-Fi сети также усугубляют проблему. Законы обязывают личным устройствам соответствовать корпоративным стандартам безопасности, что вызывает вопросы о конфиденциальности и ответственности в случае компрометации данных.

Чтобы обеспечить безопасность, необходим комплексный подход, который включает технические решения и четко сформулированные политики BYOD. Эти меры должны быть сбалансированы так, чтобы защищать корпоративные данные и уважать личную жизнь сотрудников.

Егоров Вадим Алексеевич,

обучающийся 4 курса Информационной безопасности НФ УУНУТ.

Научный руководитель: А.Р. Аюпова, к.ф.-м.н., доцент кафедры

математического моделирования и информационной безопасности

Нефтекамского филиала Уфимского университета науки и технологий,

г. Нефтекамск

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ДАННЫХ ПРИ ПРОВЕДЕНИИ ТЕСТИРОВАНИЯ СРЕДСТВАМИ GOOGLE ФОРМ

В настоящий момент, при необходимости проведения проверки знаний, опросов, анкетирования, сбора информации все больше и больше пользователей предпочитают использовать онлайн-сервисы. Но в чем же заключается преимущество современных онлайн-сервисов над другими способами?

В первую очередь следуют отметить простоту и удобство данных онлайн-сервисов, возможность вносить правки в сами вопросы и ответы к ним, настраивать внешний вид, перемешивать вопросы и варианты ответов, а также управлять сбором и защитой формы. Еще одним из главных преимуществ онлайн-

ресурсов является автоматический сбор и анализ полученных результатов с дальнейшим экспортом в другие приложения и источники. Разобравшись с главными преимуществами данных сервисов следует перейти к наиболее популярным решениям онлайн-сервисов, в которых возможно проведение тестирования:

1. МТС Линк Формы – это сервис, который позволяет создавать формы и управлять ими для сбора информации от пользователей. Здесь можно создать тест, анкету, опрос, квиз или викторину. МТС Линк Формы пока работает в режиме раннего доступа и является относительно новым на рынке²⁹.

2. Google Forms – это онлайн-инструмент, позволяющий создавать формы для сбора данных, онлайн-тестирования и голосования. Чаще всего Формы используются для опроса клиентов или проведения тестирования среди студентов и школьников³⁰.

3. Online Test Pad – еще один сетевой ресурс, позволяющий бесплатно создавать интерактивные задания для использования их в учебном процессе. Online Test Pad предлагает довольно ограниченный набор типов учебных заданий, среди которых Online Test Pad:

- позволяет создавать три вида тестов: образовательные, психологические и развлекательные;

- дает возможность создавать и проводить онлайн-опросы на различные темы, получать статистику ответов;

- позволяет создавать кроссворды различных видов (классические, сканворды, судоку), пользователь может создавать онлайн-кроссворды различных размеров и форм, внести в них любое количество слов по своему желанию;

- предлагает разнообразные варианты логических игр, составленных из слов из букв, фраз из слов, разгадывание загадок и ребусов³¹.

4. Yandex Forms – это сервис, где можно проводить опросы, тесты и квизы, собирать отзывы и принимать заявки. В Yandex Forms доступны разные типы вопросов, из которых легко составить любой опрос или тест. Форму можно разместить на сайте или поделиться с пользователями по ссылке³².

²⁹ Едакин А. Обзор МТС Линк Форм – сервиса для создания тестов, опросов и квизов // MTS-Link.ru. 2025. URL: <https://mts-link.ru/blog/obzor-mts-link-form-servisa-dlya-sozdaniya-testov-oprosov-i-anket/#z1> (дата обращения: 10.04.2025).

³⁰ Google. Обзор Google Forms // Google.ru. 2025. URL: <https://www.google.ru/intx/ru/forms/about/#features> (дата обращения: 10.04.2025).

³¹ Локишина Ю. Методические рекомендации по работе с конструктором интерактивных заданий Online Test Pad (образовательные тесты) // otdis.ru. 2019. URL: <https://www.otdis.ru/upload/iblock/550/vtprfnp3e9b0f9itsq9pnfdngmbkm8kn4.pdf> (дата обращения: 10.04.2025).

³² Yandex. Обзор сервиса Forms // Yandex.ru. 2025. URL: <https://yandex.ru/support/forms/ru/overview> (дата обращения 10.04.2025).

5. Madtest – является интерактивным конструктором для создания квиз-тестов. Madtest обладает защитой от списывания, возможностью интеграции и обменом информации с другими сервисами и приложениями.

Среди вышеописанных, сервисов наиболее популярным и удобным является Google Forms от компании Google. Данный сервис выбирают за имеющуюся инфраструктуру Google Workspace, в которой возможна работа и обработка любой информации и что самое главное из-за его банальной простоты, с интерфейсом которого сможет разобраться любой пользователь.

Google Forms уже обладает достаточно надежной защитой и гибкой её настройкой без участия автора, но если обрабатываются персональные данные или конфиденциальные сведения, тогда стоит особенно хорошо задуматься об обеспечении безопасности. Так обеспечение безопасности можно разделить на то, что зависит от пользователя и на то, что уже используется в Google Forms. За информационную безопасность сервисов в Google отвечает команда разработчиков Project Zero.

В Google любой передаваемый трафик и данные надежно защищены с помощью протоколов HTTPS и TLS. Также в Google имеется комплексная стратегия безопасности, которая включает шифрование данных, что помогает защитить данные клиентов от злоумышленников. Google шифрует весь контент своих клиентов в состоянии покоя без каких-либо действий со стороны пользователя, используя один или несколько механизмов шифрования. Все данные, хранящиеся в Google, шифруются на уровне хранения с использованием алгоритма Advanced Encryption Standard (AES), AES-256, а также используя криптографическую библиотеку Tink, которая включает модуль FIPS 140-2³³. В Google Workspace также имеются журналы аудита, благодаря которым ведется постоянная фиксация всех необычных поведений пользователя.

Теперь можно перейти к действиям, которые может сделать сам пользователь, чтобы обеспечить большую безопасность данных. С первым с чем сталкивается любой пользователь – это создание пароля. В данной статье не будет уделяться много внимания правилам использования надежных паролей. Но каким бы сложным и длинным ни был пароль, более надежную защиту сможет обеспечить двухфакторная аутентификация (2FA). Благодаря 2FA удастся заблокировать до 99,9 % всех автоматизированных кибератак. В Google 2FA возможна, начиная от текстового подтверждения до специальных ключей безопасности.

³³ Google. Default encryption at rest // Cloud.Google.com. 2025. URL: <https://cloud.google.com/docs/security/encryption/default-encryption> (дата обращения: 10.04.2025).

Теперь можно перейти к защите самой формы, сделать это можно установив пароль в начале формы, как показано на рисунке 1.

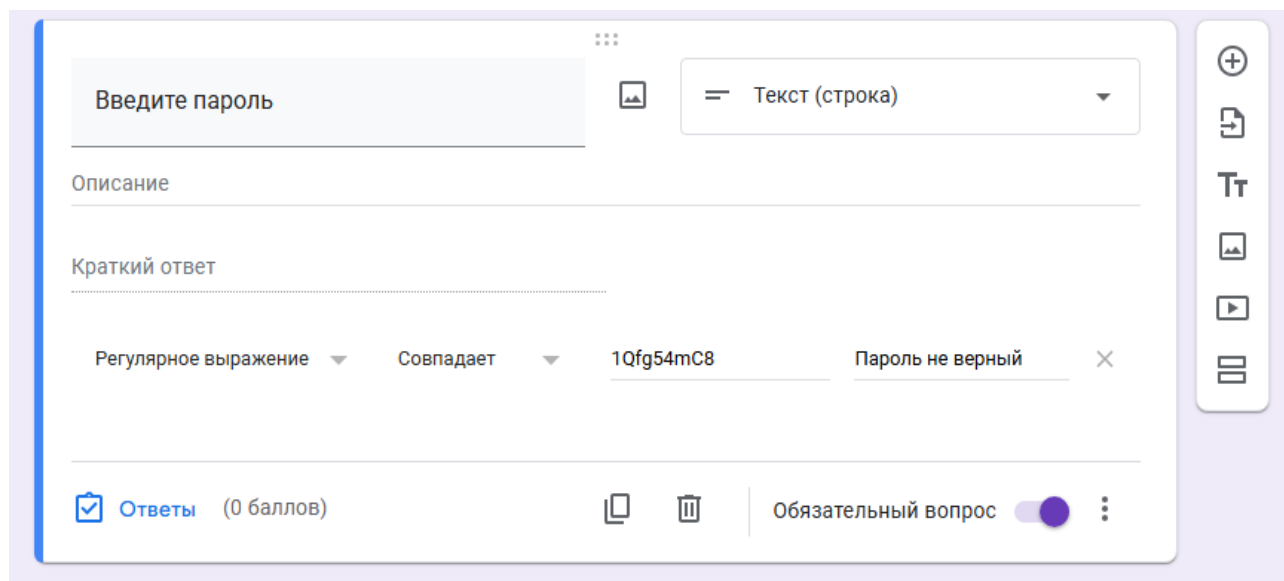


Рис. 1. Создание поля с паролем в Google Forms.

Данное поле с паролем, позволит ограничить доступ к форме, обеспечив, что собранные сведения будут являться достоверными и получены только от опрашиваемых пользователей, исключив спам-ботов. Также можно свести к минимуму сбор чувствительных и персональных данных опрашиваемых пользователей.

Но, казалось бы, даже у такой весьма крупной и серьезной компании как Google были сбои и утечки данных. Так в 2018 году в социальной сети Google+ непреднамеренно предоставила разработчикам приложений доступ к персональным данным около 53 миллионов пользователей. У разработчиков был доступ к имени, дате рождения, адрес электронной почты и истории трудовой деятельности пользователей. Данная ошибка просуществовала 6 дней и привела к утечке почти 500 тыс. аккаунтов пользователей. Вскоре после данного случая компания Google приняла решение закрыть свою социальную сеть.

В заключении можно сказать, что Google Forms являются самым популярным, удобным и безопасным вариантом для большинства пользователей. Google Forms обеспечивает защиту данных, с помощью шифрования, двухфакторной аутентификации, контроля доступа и журнала аудита. Компания Google предлагает обширный набор инструментов для обеспечения защиты данных, но сами пользователи также должны следовать рекомендациям и быть внимательными, так как итоговая защита лежит за автором.

**Желнин Алексей Михайлович,
Новосельских Дмитрий Алексеевич,**

*обучающиеся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».*

*Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры
информационной безопасности в управлении Удмуртского
государственного университета,
г. Ижевск*

СОЗДАНИЕ ПРИЛОЖЕНИЯ ДЛЯ ОПОВЕЩЕНИЯ ГРАЖДАН О ПРАВОНАРУШЕНИЯХ

Современные города сталкиваются с множеством проблем, связанных с общественной безопасностью, включая рост правонарушений, нарушения общественного порядка и преступности. Важно, чтобы граждане могли не только быстро реагировать на происходящее, но и делиться информацией с другими, создавая тем самым сообщество, которое активно помогает обеспечивать безопасность. В условиях цифровизации и повсеместного использования мобильных устройств появляется реальная возможность сделать процесс мониторинга правонарушений более эффективным и доступным для широкой аудитории.

Данный проект направлен на решение одной из таких проблем – обеспечению безопасности через использование мобильных технологий. Возможность для граждан фиксировать правонарушения и делиться этой информацией с другими людьми в реальном времени позволяет создать платформу для взаимодействия, которая будет способствовать повышению осведомленности и быстрому реагированию на правонарушения.

Целью проекта является создание мобильного приложения для платформы Android, которое позволит пользователям сообщать о правонарушениях, фиксировать их на фото, указывать точные координаты происшествия и делиться этой информацией с другими пользователями. Приложение должно стать инструментом для активного участия граждан в обеспечении общественного порядка и безопасности.

Задачи проекта:

1. Разработка функционала для добавления правонарушений.

2. Разработка системы уведомлений.
3. Обеспечение безопасности и конфиденциальности данных.
4. Внедрение аналитики для анализа правонарушений.
5. Обеспечение удобства и доступности для широкого круга пользователей.

Приложение направлено на улучшение общественной безопасности, предоставляя гражданам платформу для обмена информацией о правонарушениях. Для правоохранительных органов это может стать дополнительным источником данных для оперативного реагирования. Однако главное – это создание активного сообщества граждан, которые помогают друг другу в защите своих прав и обеспечении безопасности в своем районе.

Как это работает? Перед началом использованием нашего приложения пользователь должен пройти обязательно регистрацию. Для этого ему нужно ввести ‘Email’ и ‘Пароль’ в соответствующие поля.

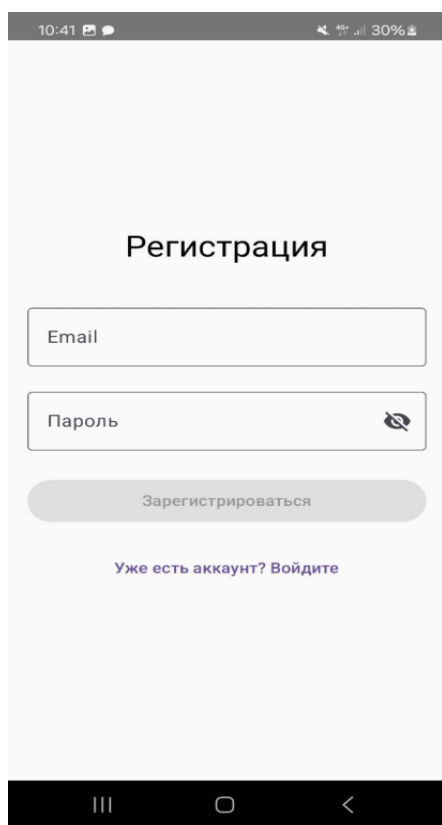


Рис. 1. Окно регистрации.

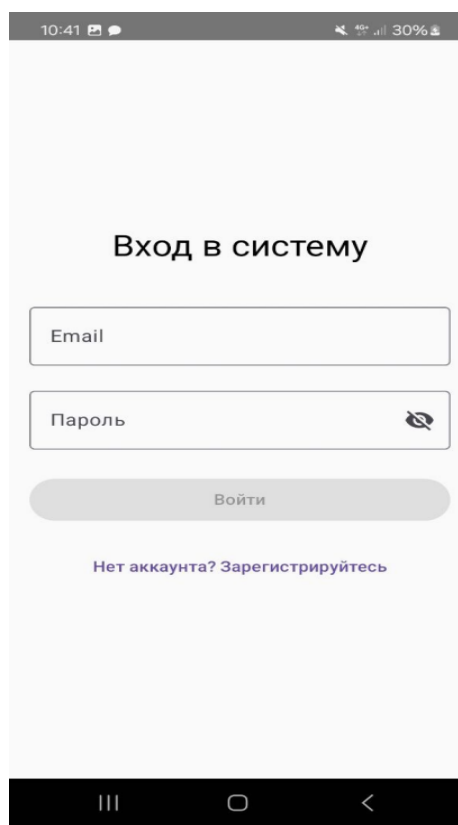


Рис. 2. Окно входа в систему.

После успешной регистрации пользователь должен авторизоваться, введя ранее использованные данные для регистрации (рис. 2). Пользователь может просматривать нарушения в режиме реального времени. Когда пользователь замечает правонарушение, он может запустить приложение и: сделать фотографию с места происшествия, указать адрес где это произошло кратко описать сам инцидент и нажать кнопку “Отправить сообщение”.

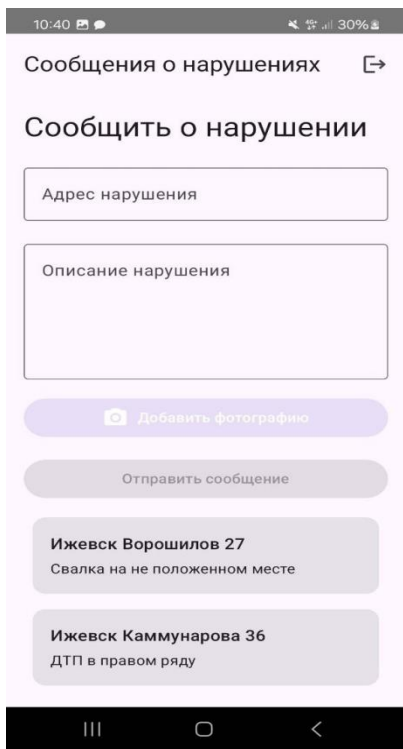


Рис. 4. Окно ввода данных о правонарушении.



Рис. 5. Пример ввода данных о правонарушении.

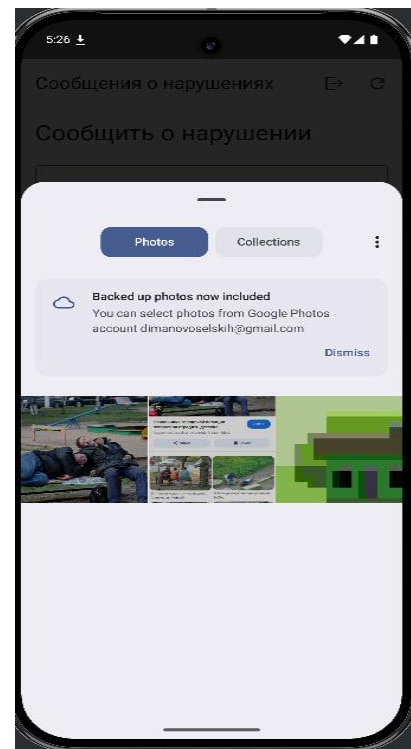


Рис. 6. Пример загрузки изображения о правонарушении.

Важным моментом является то, что это приложение работает в реальном времени. Чем больше людей используют приложение, тем быстрее можно распространять информацию о правонарушениях и тем более эффективной будет реакция общественности

Куда может отправляться эта информация? Полиция: Для оперативного расследования правонарушений, таких как кражи, насилие, нарушения общественного порядка и другие преступления. Федеральная служба по контролю за наркотиками (ФСКН): Для сообщений о правонарушениях, связанных с незаконным оборотом наркотиков. Госавтоинспекция (ГИБДД): Для фиксации нарушений правил дорожного движения, таких как превышение скорости, управление транспортным средством в нетрезвом состоянии, неправильная парковка и другие. Миграционная служба: Для информации о правонарушениях, связанных с нарушением миграционного законодательства. Администрация города: Для информации о правонарушениях, которые касаются местных правил и норм (например, незаконная торговля, несанкционированные свалки, незаконное строительство). Жилищные инспекции: Для сообщений о нарушениях, связанных с жилищными правами, плохими условиями проживания, нарушением санитарных норм в жилых зданиях. Роспотребнадзор: Для сообщений о правонарушениях в сфере защиты прав потребителей, нарушениях санитарных норм, использования несертифицированной продукции и других вопросов, связанных с безопасностью здоровья граждан.

Приложение разработано с использованием языка программирования Kotlin – это современный, но уже зрелый язык программирования, призванный сделать разработчиков счастливее. Он лаконичен, безопасен, совместим с Java и другими языками и предоставляет множество способов повторного использования кода между несколькими платформами для продуктивного программирования³⁴.

Важными особенностями нашего приложения являются: интерфейс: Мы старались создать интуитивно понятный и простой интерфейс, чтобы пользователи могли быстро разобраться, как добавить правонарушение или найти информацию.

Реализация базы данных: Для хранения данных о правонарушениях использована база данных Supabase предоставляет полноценную базу данных для каждого проекта с функцией работы в реальном времени, резервными копиями баз данных, расширениями и многим другим. Она предоставляет набор инструментов для работы с базами данных, аутентификацией, хранением файлов и функциями в реальном времени. Supabase основан на PostgreSQL и включает в себя автоматическую генерацию API, что позволяет разработчикам быстро интегрировать функциональность в свои приложения без необходимости настраивать серверы или базы данных вручную³⁵.

Особое внимание было уделено вопросам безопасности и конфиденциальности данных. Все фотографии и описания правонарушений проходят проверку, чтобы исключить возможность злоупотреблений. Также в приложении предусмотрены настройки конфиденциальности, позволяющие пользователю контролировать, какие данные он готов делиться.

Вход через Google почту – доступ в приложение осуществляется с использованием учетной записи Google, что упрощает процесс регистрации и повышает безопасность.

Приложение не сохраняет личные данные пользователей без их разрешения, и все взаимодействия с ним анонимны, что минимизирует риски.

Это приложение – лишь первый шаг в развитии платформы для гражданского мониторинга правонарушений. В будущем планируется добавить следующие функции:

Интеграция с правоохранительными органами: Возможность оперативной передачи информации о правонарушениях в правоохранительные органы для быстрого реагирования.

³⁴ О программировании на языке Kotlin. URL: <https://kotlinlang.org/> (дата обращения: 10.04.2025).

³⁵ Об использовании базы данных supabase. URL: <https://supabase.com/> (дата обращения: 12.04.2025).

Аналитика: Система аналитики, которая позволит выявлять тенденции и «горячие точки» правонарушений, что поможет в принятии мер для повышения безопасности.

Интеграция с Яндекс.Картами API: В перспективе мы планируем интеграцию с Яндекс.Картами API для отображения правонарушений на интерактивной карте. Это позволит улучшить навигацию для пользователей

Мы уверен, что это приложение может сыграть важную роль в обеспечении безопасности и правопорядка в нашей стране. Оно даёт возможность каждому человеку быть не просто свидетелем, но и активным участником в борьбе с правонарушениями.

Пользователи, объединяясь в рамках такого приложения, смогут быстрее реагировать на возникающие проблемы, помогать правоохранительным органам и обеспечивать собственную безопасность. Надеюсь, что в будущем это приложение станет важной частью общественной безопасности и поможет в решении множества социальных вопросов.

**Кагарманов Аделий Ренатович,
Исупов Рустам Салохиддинович,**

*обучающиеся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».*

*Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры
информационной безопасности в управлении Удмуртского
государственного университета,
г. Ижевск*

ИССЛЕДОВАНИЕ LC-АВТОГЕНЕРАТОРА ГАРМОНИЧЕСКИХ КОЛЕБАНИЙ

LC-автогенератор – это электронное устройство, которое генерирует незатухающие гармонические колебания на определенной частоте. Его основу составляет колебательный контур, состоящий из катушки индуктивности L и конденсатора C . Благодаря этому контуру автогенератор способен поддерживать колебания за счет положительной обратной связи³⁶.

³⁶ Довгун В.П. Электротехника и электроника: учеб. Пособие : в 2-х ч. Ч. 2. Красноярск : ИПЦ КГТУ, 2006. С. 30.

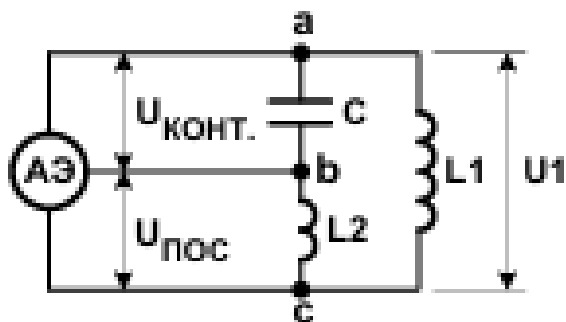
Основное назначение LC-автогенераторов – формирование стабильных синусоидальных сигналов, которые широко используются в радиотехнике, телекоммуникациях, медицинской аппаратуре и других областях.

Колебательный контур LC является ключевым элементом автогенератора. В нем энергия периодически перетекает между магнитным полем катушки и электрическим полем конденсатора. Это создает гармонические колебания, которые можно использовать для передачи информации или как эталонные сигналы.

Однако важно отметить, что реальный колебательный контур всегда имеет активное сопротивление R, которое приводит к затуханию колебаний. Для компенсации этих потерь используется активный элемент (например, транзистор или операционный усилитель), который усиливает сигнал и возвращает его в контур через положительную обратную связь.

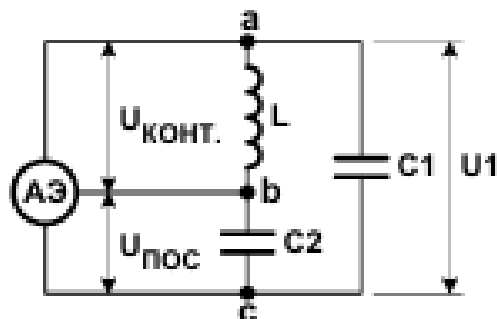
Наибольшее распространение получили две схемы LC-автогенераторов, первая имеет название индуктивной трехточки (или автотрансформаторная) – рис. 1, вторая емкостной трехточки – рис. 2.

Автогенераторы рис. 1 и рис. 2 относятся к классу генераторов с минимальной связью. В схеме индуктивной трехточки (рис. 1) используется резонансная система параллельный контур второго вида, а в схеме емкостной трехточки (рис. 2) параллельный контур третьего вида³⁷.



$$L=L1+L2, fr = \frac{1}{2\pi\sqrt{LC}}$$

Рис. 1. Индуктивная трехточка.



$$C = \frac{C1 \cdot C2}{C1 + C2} \quad fr = \frac{1}{2\pi\sqrt{LC}}$$

Рис. 2. Емкостная трехточка.

Колебательный контур состоит из катушки индуктивности L и конденсатора C. При зарядке конденсатора он накапливает электрическую энергию, которая затем преобразуется в магнитную энергию в катушке индуктивности. Этот процесс повторяется, создавая гармонические колебания. Частота этих колебаний определяется формулой Томсона.

³⁷ Баскаков С.И. Радиотехнические цепи и сигналы. Руководство к решению задач : учеб. пособие для радиотехн. спец. Вузов. Москва : Высшая школа, 1987. С. 79.

$$f_0 = \frac{1}{2\pi\sqrt{LC}}$$

где L – индуктивность катушки, C – емкость конденсатора.

Однако в реальности из-за наличия активного сопротивления (R) в контуре колебания затухают. Чтобы предотвратить это, необходимо добавить внешний источник энергии, который будет компенсировать потери.

Положительная обратная связь – это механизм, при котором часть выходного сигнала возвращается на вход устройства в фазе с исходным сигналом. Это усиливает сигнал и обеспечивает его самоподдержание³⁸.

В LC-автогенераторе обратная связь организуется через специальные элементы (например, делитель напряжения или трансформатор), которые передают часть сигнала с выхода на вход. Это позволяет компенсировать потери энергии в контуре.

Для успешного запуска автогенератора должны выполняться два условия: амплитудное и фазовое.

Амплитудное условие: коэффициент усиления системы должен быть больше или равен единице. Это означает, что сигнал, возвращаемый через обратную связь, должен быть достаточным для компенсации потерь.

Фазовое условие: суммарный фазовый сдвиг сигнала в контуре должен быть кратен 2π , чтобы обеспечить синфазность входного и выходного сигналов. Это гарантирует, что сигналы будут складываться конструктивно, усиливая друг друга.

Если эти условия не выполняются, колебания либо затухнут, либо вообще не начнутся.

Различают мягкий и жесткий режимы самовозбуждения. В мягком режиме начальное смещение транзистора находится на линейном участке характеристики, и колебания плавно нарастают при увеличении коэффициента обратной связи. В жестком режиме смещение близко к напряжению отсечки, и для запуска требуется значительная обратная связь.

В программе Micro cap была собрана схема (см. рис. 3 на стр. 64) LC-автогенератора с трансформаторной обратной связью для исследования мягкого и жесткого режимов самовозбуждения.

³⁸ Хоровиц П., Хилл У. Искусство схемотехники : пер. с англ. 6-е изд. Москва : Мир, 2003. С. 45.

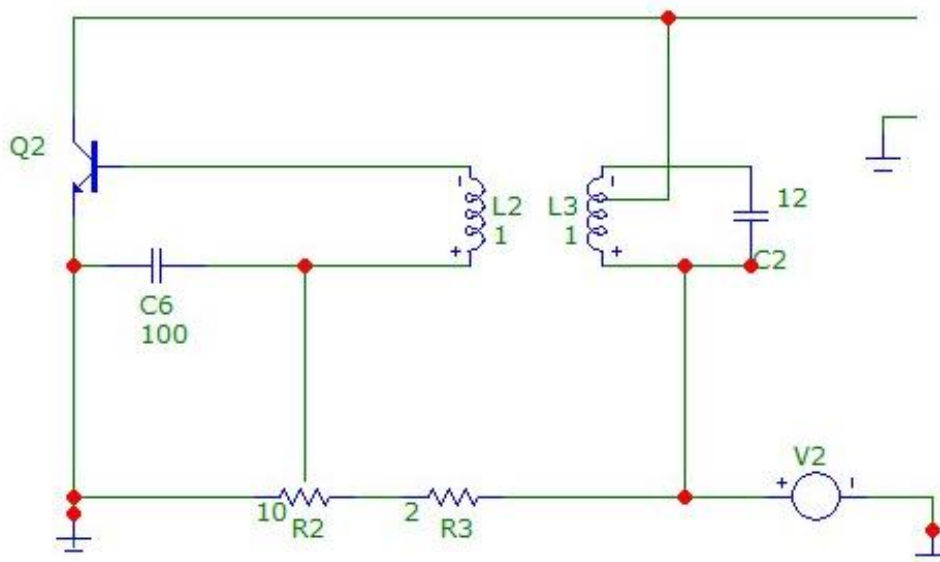


Рис. 3. Схема LC-автогенератора.

На основе данных из таблицы был построен график мягкого режима самовозбуждения (рис. 4).

Таблица 1

Параметр	Обозначение	Значение
Сопротивление R1	R1	1 кОм
Сопротивление R2	R2	10 кОм
Взаимная индуктивность	M	0.5 мкГн
Напряжение смещения Uб	Uб	0.7 В
Напряжение питания	Vc	12 В

Начальное смещение транзистора находится на линейном участке характеристики, и колебания плавно нарастают при увеличении коэффициента обратной связи.

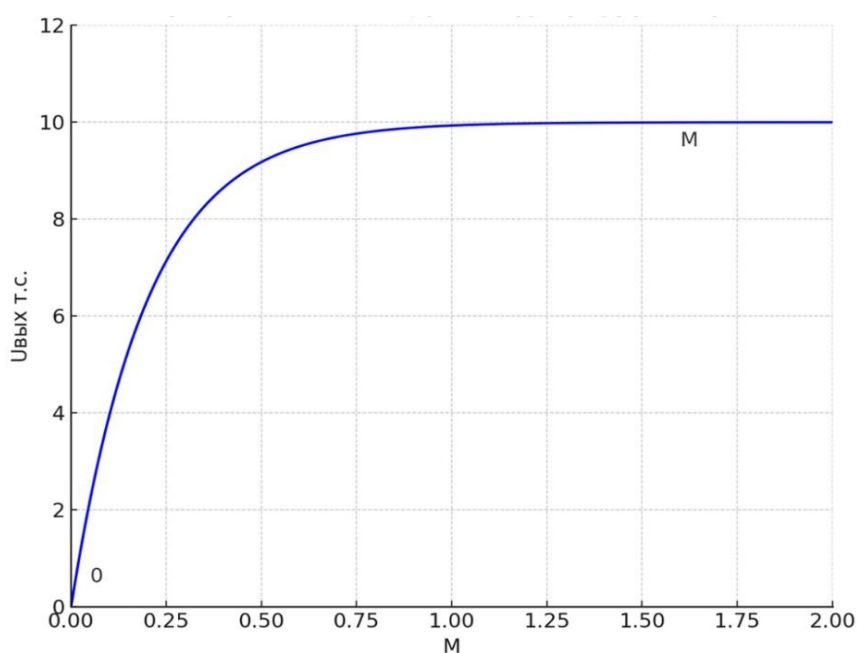


Рис. 4. Мягкий режим самовозбуждения.

На основе данных из таблицы был построен график жесткого режима самовозбуждения (рис. 5).

Таблица 2

Параметр	Обозначение	Значение
Сопротивление R1	R1	500 Ом
Сопротивление R2	R2	50 кОм
Взаимная индуктивность	M	1.2 мкГн
Напряжение смещения Uб	Uб	0.3 В
Напряжение питания	Vс	12 В

Смещение близко к напряжению отсечки, и для запуска требуется значительная обратная связь; после возникновения колебаний коэффициент обратной связи можно уменьшить.

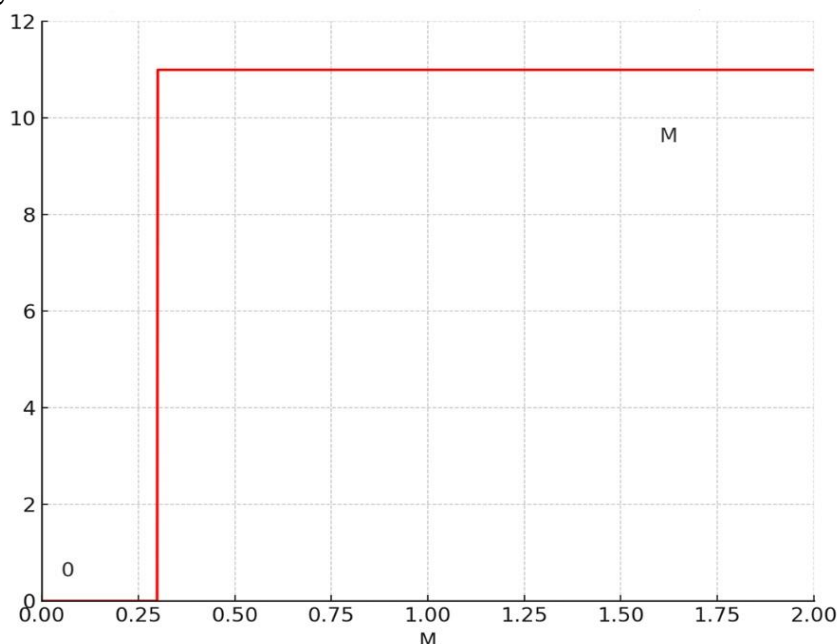


Рис. 5. Жесткий режим самовозбуждения.

LC-автогенератор гармонических колебаний – это фундаментальное устройство, которое лежит в основе многих современных технологий. Его работа основана на простых, но мощных физических принципах, таких как резонанс в колебательном контуре и положительная обратная связь.

В ходе исследования LC-автогенератора гармонических колебаний были изучены два ключевых режима самовозбуждения: мягкий и жёсткий. Выбор режима зависит от требований к стабильности и условиям запуска. Мягкий режим подходит для систем с плавным стартом, жёсткий – для устройств, где необходима устойчивость к случайным помехам или управляемый запуск.

Настройка параметров позволяет контролировать частоту генерации и динамику переходных процессов.

Проведённый анализ подтверждает, что понимание механизмов самовозбуждения и корректный подбор параметров схемы являются основой для создания эффективных и надёжных LC-автогенераторов.

Коноплёв Артём Андреевич,

обучающийся 2 курса магистратуры

Инженерно-технологического института ФГБОУ ВО

«Государственный аграрный университет Северного Зауралья».

Научные руководители: И.В. Савчук, к.т.н., доцент, доцент кафедры

энергообеспечения сельского хозяйства; Т.А. Широбокова, к.т.н., доцент

ФГБОУ ВО «Государственный аграрный университет Северного Зауралья»,

г. Тюмень

ПРОВЕДЕНИЕ ИСПЫТАНИЙ СИЛОВЫХ КАБЕЛЕЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Информационная безопасность компании, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных³⁹. Безопасность информационной инфраструктуры компании подразумевает защиту от случайных или умышленных действий, которые могут нанести вред владельцам данных или их пользователям. Действия лиц, несущих ответственность за эту сферу, должны быть направлены на создание защиты, препятствующей утечкам данных, а не борьбу с их последствиями.

Одним из опасных технических каналов утечки информации на объектах является канал утечки информации, появляющийся в результате дефектов изоляции силовых кабелей, так как из-за них в окружающую среду излучаются электромагнитные волны, несущие в себе информацию о работе объекта.

Это происходит из-за частичных разрядов, которые возникают во включениях в изоляции, например, в газовых включениях или по водным триингам. Такие разряды генерируют импульсные электрические сигналы, которые распространяются по электрически связанным цепям⁴⁰.

³⁹ Почему важна информационная безопасность организации и методы ее обеспечения. URL: <https://bitcop.ru/blog/informacionnaya-bezopasnost-organizacii>

⁴⁰ Чухланцев Г.М., Стерхова Т.Н. Значение информационной безопасности в области электроэнергетики // Менеджмент безопасности жизнедеятельности: перспективы развития и проблемы преподавания : сборник материалов IV открытой Республиканской научно-практической интернет-конференции, Минск, 13 декабря 2022 года. Минск : Университет гражданской защиты Министерства по чрезвычайным ситуациям Республики Беларусь, 2023. С. 155–158.

Некоторые факторы, оказывающие влияние дефектов изоляции на утечку информации: загрязнённая и увлажнённая поверхность изоляционного тела, воздушные включения.

Надёжность электроснабжения, особенно в условиях сурового климата, играют ключевую роль в обеспечении продовольственной безопасности страны. Электрические системы включают в себя не только системы отопления и вентиляции, освещение, системы автоматического контроля климата и другие технологические процессы. Любые перебои в подаче электроэнергии могут привести к быстрой порче продукции, значительным экономическим потерям и даже полному уничтожению запасов. Поэтому гарантированная надёжность и безопасность электроснабжения – это необходимость⁴¹.

В 2024 году на агропромышленном предприятии Упоровского района Тюменской области были проведены испытания силовых кабелей марки ВВГнг-LS и сечением 4x240мм². Основной задачей проверки было выявление дефектов в изоляции и анализ его работоспособности при высоких нагрузках⁴².

Для проведения испытаний силового кабеля ВВГнг-LS был использован прибор для измерения сопротивления изоляции «Мегаомметр Е6-24» с диапазоном измерения 2500±125 В и погрешностью ±1,5 % от шкалы равной 88 мм.

1. Непосредственно перед измерением необходимо обесточить кабель и убедиться, что жилы не замкнуты накоротко.

2. Убедиться в отсутствии остаточного заряда, разрядив кабель через заземление.

3. Очистить поверхность изоляции кабеля от пыли, влаги и загрязнений, чтобы исключить влияние внешних факторов на измерение.

4. Проверить исправность мегаомметра Е6-24, проведя самотестирование и установив необходимое тестовое напряжение.

Порядок проведения измерения.

1. Подключение прибора.

Так как испытываемый кабель многожильный, измерения проводятся поочерёдно для каждой жилы относительно земли и между жилами.

2. Выбор испытательного напряжения.

Для кабелей с номинальным напряжением до 1000 В и сечением более 16 мм² на приборе выставляется напряжение 2500 В.

⁴¹ Будзко И.А., Лецинская Т.Е., Сукманов В.И. Электроснабжение сельского хозяйства. Москва : Колос, 2000.

⁴² Широбокова Т.А. Разработка энерго-ресурсосберегающих осветительных установок для АПК / И.Г. Поспелова, М.А. Набатчикова, И.И. Иксанов. Москва : Федеральный научный агроинженерный центр ВИМ., 2020.

3. Проведение измерения.

Включается подача тестового напряжения, и через несколько секунд фиксируется показание прибора. Ожидается стабилизация показаний (обычно 15–60 секунд), после чего записывается значение сопротивления изоляции.

Если прибор показал значения сопротивления изоляции не менее 0,5 Мом, кабель соответствует требованиям ПУЭ-7 глава 1.8 нормы приёмо-сдаточных испытаний.

Таблица 1

Значения сопротивления изоляции.

№ п/п	Наименование испытываемой электроустановки (присоединения, линии)	Испыт. напряж., В	Сопротивления изоляции (МОм)							Вывод (соотв., не соотв.)
			L1+L2 L3+N	L1+L3 L2+N	L2+L3 L1+N	L1 Pe (Броня)	L2 Pe (Броня)	L3 Pe (Броня)	N Pe (Броня)	
	КТП-10/0,4кВ									
1	QF1, ВВГнг(А)-LS 4x240	2500	1380	1150	1370	1210	1320	1190	1160	Соотв.
2	QF2, ВВГнг(А)-LS 4x240	2500	1350	1050	1100	1220	1390	1200	1080	Соотв.

4. Отключение и разрядка кабеля. После измерений кабель обязательно разряжается через заземление или же через мегаомметр, чтобы избежать накопленного заряда.

Затем прибор отключается, а кабель возвращается в эксплуатацию при удовлетворительных результатах теста.

На основе полученных данных можем сделать вывод, что силовые кабели марки ВВГнг(А)-LS и сечением 4x240 мм² соответствуют нормам ПУЭ-7 глава 1.8 нормы приёмо-сдаточных испытаний. Следовательно, использование испытываемых кабелей обеспечивает не только надежность работы силового оборудования, но и утечку информации о техническом состоянии производственного объекта.

Кутергин Данил Сергеевич,
Шамшурина Анастасия Андреевна,

*обучающиеся 3 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».*

*Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры
информационной безопасности в управлении Удмуртского
государственного университета, г. Ижевск*

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ДЛЯ АВТОМАТИЗАЦИИ ПРОЕКТИРОВАНИЯ ЦИФРОВЫХ ФИЛЬТРОВ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Цифровые фильтры: сравнительный анализ FIR и IIR фильтров и их применение в системах обработки сигналов.

В современной цифровой обработке сигналов (ЦОС) особое место занимают два основных типа фильтров: FIR (Finite Impulse Response – фильтры с конечной импульсной характеристикой) и IIR (Infinite Impulse Response – фильтры с бесконечной импульсной характеристикой). Эти фильтры принципиально отличаются по своим характеристикам и областям применения, что делает их выбор важным этапом при проектировании систем обработки сигналов.

FIR-фильтры характеризуются конечной длительностью импульсной характеристики, что означает полное затухание сигнала через определенное количество тактов. Основными преимуществами FIR-фильтров являются:

1. Гарантированная устойчивость, так как они не используют обратную связь.
2. Линейная фазовая характеристика, что особенно важно для приложений, где требуется сохранение формы сигнала.
3. Простота проектирования и реализации.

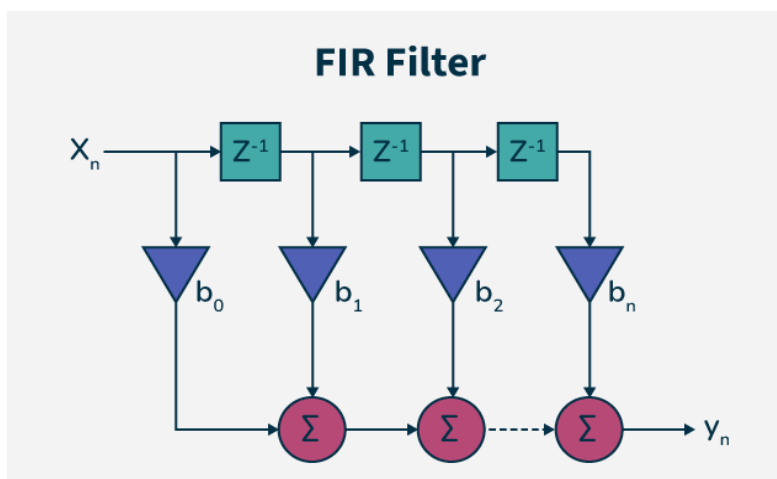


Рис. 1. Упрощенная схема FIR-фильтра.

4. Отсутствие проблем с переполнением разрядной сетки.

Однако FIR-фильтры требуют большего количества коэффициентов (и, соответственно, вычислительных ресурсов) для достижения характеристик, сравнимых с IIR-аналогами. Это делает их менее эффективными для приложений реального времени с жесткими требованиями к быстродействию⁴³.

В практических приложениях выбор между FIR и IIR фильтрами зависит от конкретных требований системы. FIR-фильтры предпочтительны в задачах, где критична линейность фазы (аудиообработка, биометрия, системы связи). IIR-фильтры находят применение в системах реального времени с ограниченными вычислительными ресурсами (анализаторы трафика, системы мониторинга).

Современные подходы к проектированию цифровых фильтров часто сочетают преимущества обоих типов, например, используя каскадное соединение FIR и IIR фильтров для достижения оптимального баланса между качеством обработки и вычислительной эффективностью. Развитие вычислительной техники и алгоритмов проектирования продолжает расширять границы применения цифровых фильтров в различных областях – от телекоммуникаций до биомедицинских систем⁴⁴.

2. Разработка приложения для проектирования цифровых фильтров: от концепции до реализации.

В современной цифровой обработке сигналов остро стоит вопрос автоматизации процессов проектирования фильтров. Представленное приложение было разработано как комплексное решение для инженеров и исследователей, позволяющее существенно упростить и ускорить процесс создания цифровых фильтров. Основой приложения стал Python 3.12 – язык, идеально подходящий для научных вычислений благодаря богатой экосистеме специализированных библиотек.

Особое внимание было уделено реализации различных методов проектирования: для FIR-фильтров это оконный метод (с поддержкой различных типов окон), метод частотной выборки и оптимальный метод Ремеза; для IIR-фильтров – билинейное преобразование и метод инвариантной импульсной характеристики с возможностью создания фильтров Баттерворта и Чебышева.

⁴³ Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов. Москва : Мир, 1978.

⁴⁴ Proakis J.G., Manolakis D.G. Digital Signal Processing: Principles, Algorithms, and Applications. Pearson, 2007.

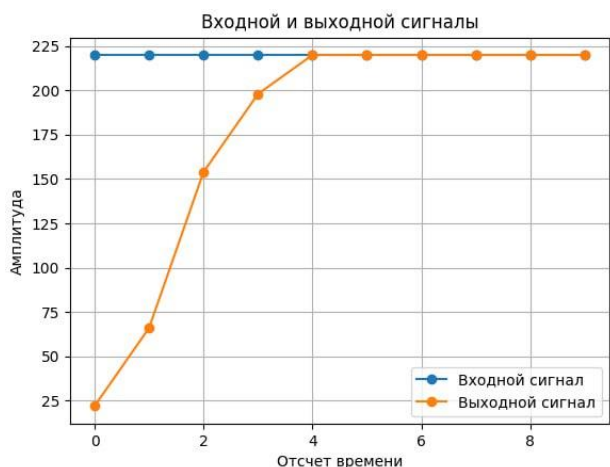


Рис. 3. График зависимости амплитуды входного и выходного сигналов от времени.

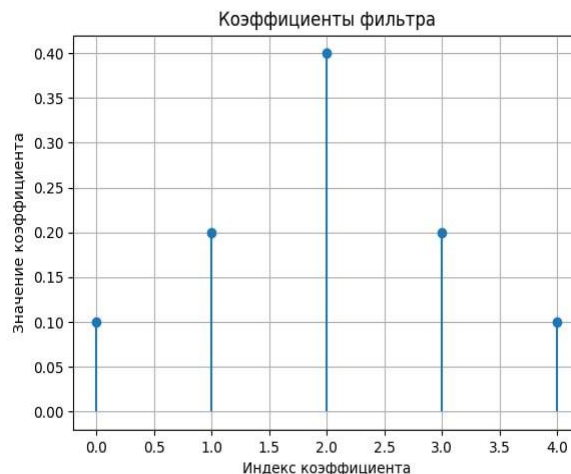


Рис. 4. График зависимости значений коэффициентов фильтра от индекса коэффициента.

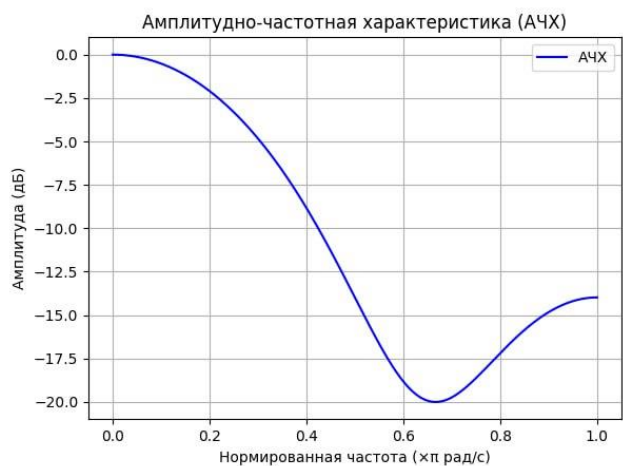


Рис. 5. График амплитудно-частотной характеристики.

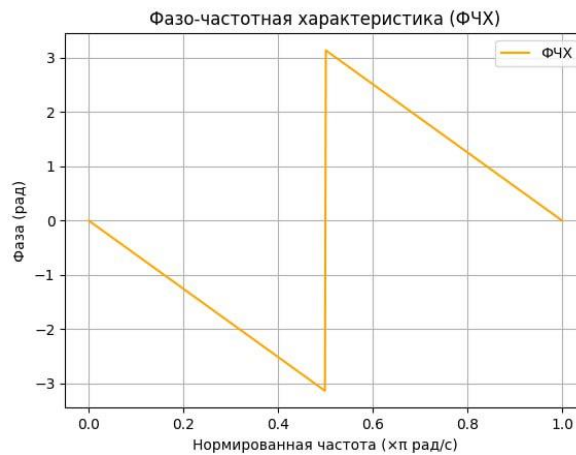


Рис. 6. График фазо-частотной характеристики.

Рисунки 3–6 показывают визуализацию программы для FIR-фильтра.

Отдельный модуль визуализации отвечает за построение и настройку графиков частотных характеристик, импульсного отклика и других параметров фильтров. Реализованные здесь функции позволяют не только отображать основные характеристики, но и сравнивать различные варианты проектирования, что особенно ценно при поиске оптимального решения⁴⁵.

Тестирование приложения проводилось на нескольких уровнях: от модульных тестов с использованием `pytest` до проверки граничных условий и сравнения результатов с эталонными реализациями.

В данной статье была рассмотрена разработка программного средства для автоматизации проектирования цифровых фильтров, ориентированного на применение в системах информационной безопасности. Проведен сравнительный анализ FIR- и IIR-фильтров, выделены их ключевые преимущества

⁴⁵ Введение в цифровую фильтрацию / под ред. А.И. Солонины. Санкт-Петербург: БХВ-Петербург, 2012.

и ограничения, а также области применения. Разработанное приложение на Python позволяет автоматизировать процесс расчета коэффициентов, визуализировать характеристики фильтров и экспортировать результаты для дальнейшего использования.

Практическая значимость работы подтверждается возможностью применения программного средства как в учебных целях, так и в реальных проектах по защите информации. Результаты демонстрируют эффективность предложенного подхода к автоматизации проектирования цифровых фильтров, что способствует повышению качества обработки сигналов и снижению временных затрат на разработку.

Павлова Злата Дмитриевна,

обучающаяся 2 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры

информационной безопасности в управлении Удмуртского

государственного университета,

г. Ижевск

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЦИФРОВЫХ ПОДСТАНЦИЯХ

Переход на цифровые технологии открывает большие возможности для автоматизации и оптимизации работы подстанций, однако влечет за собой серьезные угрозы, связанные с безопасностью данных и функционированием всей энергосистемы. Я буду рассматривать основные типы угроз, особенности построения и функционирования цифровых подстанций, а также существующие и перспективные методы защиты.

Цель: выявление угроз для цифровых подстанций и разработка рекомендаций по внедрению комплексной системы защиты информации (КСЗИ) в электроэнергетике.

Задачи:

1. Классификация угроз и рисков для цифровых подстанций.
2. Анализ современных методов защиты информации.
3. Создать пошаговую методику внедрения модели КСЗИ в цифровые подстанции.

Цифровая подстанция объединяет традиционные электротехнические устройства с современными средствами измерения, коммутации и управления, построенными на базе микроконтроллерных технологий и высокоскоростных каналов связи⁴⁶. Основными элементами цифровой подстанции являются:

- Интеллектуальные электронные устройства (IED).
- Микропроцессорная техника.
- SCADA-системы (диспетчерское управление и сбор данных).

Эти компоненты формируют сложную информационную структуру, соединяя производственные процессы и управление в единый технологический контур. Подобная архитектура повышает гибкость и функциональность подстанции, позволяя централизованно управлять всеми процессами и обеспечивая удалённый доступ к оборудованию.

Угрозы информационной безопасности

Переход на цифровые технологии увеличивает число факторов, угрожающих стабильности и безопасности подстанций. Среди главных угроз выделяются следующие группы:

1. Нарушение конфиденциальности данных: Утечка информации о работе оборудования и планах технического обслуживания может быть интересна конкурентам. Методы защиты включают криптографию, защищённые каналы передачи данных и ограничение доступа к чувствительной информации.

2. Кибератаки и отказоустойчивость: Угрозы DoS/DDoS-атак могут привести к временным отключениям оборудования, как это произошло в марте 2019 года в Калифорнии, Юте и Вайоминге. Защита включает фильтрацию пакетов, разделение сетей и мониторинг трафика.

3. Внутренние угрозы и человеческий фактор: Халатность работников и ошибки в настройках могут вызвать серьёзные проблемы. Решения: разграничение полномочий, регулярные проверки конфигураций и повышение квалификации персонала.

Методы защиты цифровых подстанций

Для эффективной защиты цифровых подстанций применяются различные методы и подходы:

1. Шифрование и аутентификация: применение криптографических методов обеспечивает защиту передаваемых данных и предотвращает несанкционированный доступ.

2. Межсетевое экранирование и сегментирование сети: создание изолированных зон позволяет минимизировать риск распространения атак внутри сети и препятствует проникновению вредоносных программ в критически важные области подстанции.

⁴⁶ ГОСТ Р МЭК 61850-5-104-2007: «Системы электроснабжения. Часть 5: Общее описание услуг и механизмов (61850-5)». Москва : Стандартинформ, 2007. С. 3.

3. Мониторинг и выявление аномалий: автоматические системы анализа активности помогают своевременно выявлять признаки вторжения и предотвращают инциденты.

4. Повышение осведомлённости персонала: регулярные тренировки и обучение сотрудников повышают уровень компетентности и снижают воздействие человеческого фактора.

Нормативно-правовая база и международные стандарты

Формирование правильной политики информационной безопасности требует учёта нормативных документов и международных стандартов. Для специалистов важны следующие положения:

– ГОСТ Р МЭК 61850 – стандарт проектирования и строительства цифровых подстанций;

– ISO/IEC 27001 – международное руководство по управлению информационной безопасностью;

– Федеральный закон № 187-ФЗ – российский норматив, регулирующий защиту информационных ресурсов и обеспечение кибербезопасности⁴⁷.

А также полезно учитывать рекомендации иностранных регуляторов.

Опыт реализации и успешные проекты

Опыт российских компаний демонстрирует положительную динамику в развитии мероприятий по защите цифровых подстанций⁴⁸. Пример успешной реализации – модернизация нескольких крупных подстанций ОАО «ФСК ЕЭС», где была реализована концепция сегментации сети и установлены специализированные системы обнаружения вторжений. Другой значимый проект – реализация проекта «Умная подстанция» ПАО «Россети». Реализованные проекты показали свою эффективность, подтвердив важность заблаговременного планирования и тщательной проработки вопросов безопасности.

Применение модели КСЗИ в цифровых подстанциях

Комплексная система защиты информации (КСЗИ) представляет собой многоуровневую архитектуру защиты.

Принцип многоуровневой защиты

Современная система защиты информации должна иметь несколько перекрывающихся уровней, чтобы злоумышленнику было сложно добраться до закрытой информации. Каждый уровень предназначен для выявления и устранения угроз. Если угроза не устраняется на одном уровне, последующие рубежи

⁴⁷ О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ // Собрание законодательства Российской Федерации. 2017. № 30, ст. 5030.

⁴⁸ Описание проектов модернизации цифровых подстанций // ФСК ЕЭС. URL: <https://www.fsk-ees.ru/> (дата обращения: 03.04.2025).

ограничивают ущерб и повышают вероятность обнаружения злоумышленника. Чем сложнее меры защиты, тем больше времени потребуется злоумышленнику для взлома, что увеличивает шансы его идентификации. Эффективность системы оценивается по времени, необходимому для преодоления всех рубежей, в течение которого служба безопасности должна обнаружить угрозу и реагировать⁴⁹.

Модель КСЗИ предусматривает выделение нескольких зон защиты:

1. Внешняя неконтролируемая зона: Территория вне АСОД без мер защиты.
2. Организационная зона: Территория предприятия, где располагается инфраструктура подстанции.
3. Зона здания: Конкретные здания, в которых размещены элементы АСОД и рабочие места персонала.
4. Помещенные зоны: помещения внутри здания, в которых расположены ресурсы автоматизированных систем и защищаемая информация. Это могут быть: служебные помещения, кабинеты, комнаты для переговоров, залы, технические помещения, склады, сейфы, шкафы и др.;
5. Каналы связи и энергоснабжения: Линии связи и электрические цепи для обмена информацией и питания.
6. Аппаратные средства: Физические устройства (серверы, терминалы, датчики и прочее), участвующие в обработке и хранении данных.
7. Программные средства: в том числе операционная система и специальные программы, осуществляющие функции защиты и тестовый контроль механизма защиты в КСЗИ.
8. Данные и носители информации: Файлы, базы данных и прочие формы хранения данных.

Каждой зоне соответствует определённая степень защиты, состоящая из четырёх этапов⁵⁰:

1. Предотвращение – доступ к информации и технологии имеет только персонал, который получил допуск от собственника информации.
2. Обнаружение – обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены.
3. Ограничение – уменьшается размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению.
4. Восстановление – обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

⁴⁹ Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. Санкт-Петербург : НИУ ИТМО, 2011. С. 24.

⁵⁰ Там же.

Таким образом, комплексная система защиты строится на сочетании физических, технических и административных мер, позволяющих обеспечить надежное хранение и обработку конфиденциальной информации.

Практическое внедрение модели КСЗИ в цифровых подстанциях

Для эффективного внедрения модели комплексной системы защиты информации (КСЗИ) в цифровых подстанциях рекомендуется следующий поэтапный подход:

1. Анализ угроз.

Провести анализ рисков и уязвимостей:

- Внешний периметр: оценка защищенности интернет-подключений и взаимодействия с третьими сторонами.
- Внутренняя инфраструктура: изучение сетевой архитектуры и определение критически важных узлов.
- Человеческие факторы: учет возможных ошибок сотрудников и недостаточной подготовки.

2. Выбор защитных мер.

Определить эффективные инструменты защиты для различных зон:

- Установка межсетевых экранов и фильтров.
- Применение двухфакторной аутентификации и строгих паролей.
- Организация физической охраны с видеонаблюдением.
- Использование ПО для мониторинга действий пользователей.

3. Физическая защита объектов.

Организация физической охраны подстанции:

- Надежные периметральные ограждения и контроль доступа.
- Системы видеонаблюдения и сигнализации.

4. Проверка и совершенствование защиты.

Регулярный анализ и проверка защитных мер:

- Технические сканирования на уязвимости.
- Тестирование протоколов передачи данных.
- Моделирование ситуаций взлома.

5. Обучение персонала.

Обеспечение высокого уровня подготовки сотрудников:

- Систематическое обучение информационной безопасности.
- Формирование корпоративной культуры ответственности.
- Обновление компетенций в области кибербезопасности.

Реализация модели КСЗИ создаст надежную многоуровневую систему защиты цифровой подстанции, снижая риски информационных инцидентов Top of Form.

Современные цифровые подстанции являются сложными технологическими комплексами, подверженными угрозам информационной безопасности. Модель КСЗИ повышает защищенность данных и надежность работы энергообъектов. Применение передовых подходов, четкое распределение ответственности и постоянное обучение сотрудников способствуют созданию безопасной среды эксплуатации.

Пархачёва Алина Андреевна,

обучающаяся 2 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: М.М. Гайсин, старший преподаватель кафедры

информационной безопасности в управлении Удмуртского

государственного университета,

г. Ижевск

ПРОГРАММА МОДЕЛИРОВАНИЯ ОЧЕРЕДИ ПО РАСПРЕДЕЛЕНИЮ ПУАССОНА

Разработанная программа предназначена для визуального моделирования работы очереди, основанной на распределении Пуассона. Данное распределение представляет собой статистическую модель, описывающую вероятность наступления определённого количества событий за фиксированный интервал времени⁵¹. В представленной системе пользователь может задавать среднее время между поступлениями и среднее время обработки, что позволяет исследовать динамику и характеристики очереди.

Программа находит применение в различных отраслях⁵²:

- управление очередями в сервисных центрах;
- анализ производственных процессов;
- оценка нагрузки в телекоммуникационных сетях.

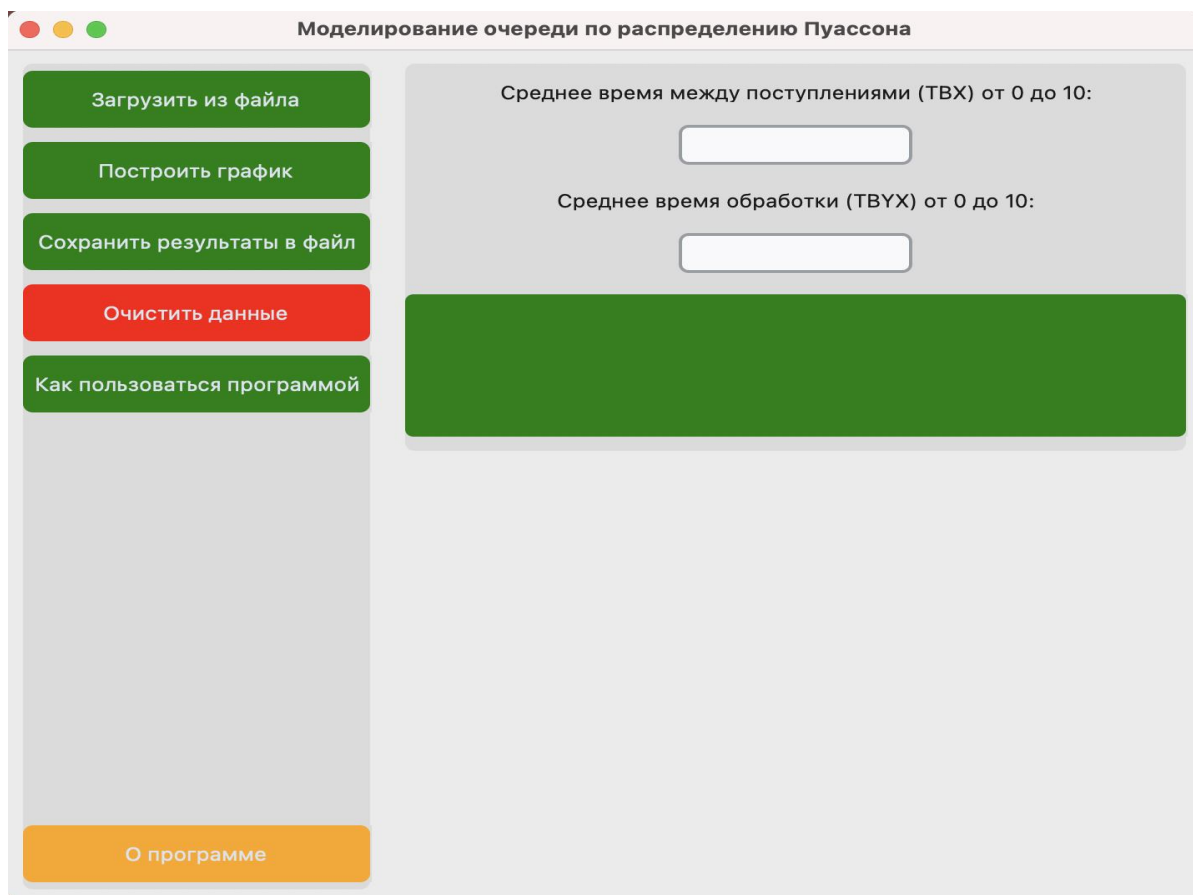
Визуализация и настройка параметров позволяют пользователю проанализировать поведение системы в различных условиях.

⁵¹ Барышева В.К., Галанов Ю.И., Ивлев Е.Т., Пахомова Е.Г. Теория вероятностей. Томск : ТПУ, 2004. С. 77.

⁵² Что такое распределение Пуассона простыми словами // Telegra. URL: <https://telegra.ph/СНто-такое-распределение-Puassona-prostymi-slovami-СНто-такое-распределение-Puassona-Pogruzhaemysya-v-mir-sluchajnyh-sobytij-07-06> (дата обращения: 13.04.2025).

Функциональные возможности:

1. Ввод исходных данных: среднее время между поступлениями и среднее время обработки.
2. Загрузка входных параметров из текстового файла.
3. Генерация и отображение графиков длины очереди во времени.
4. Сохранение результатов моделирования в текстовом файле и графике в формате PNG.
5. Интуитивно понятный графический интерфейс с кнопками управления.



Пример применения.

Для наглядности можно представить автобусную остановку. Требуется спрогнозировать, сколько автобусов прибудет в течение часа⁵³. Решение этой задачи возможно посредством распределения Пуассона, позволяющего оценить вероятность наступления определённого количества событий (в данном случае – прибытия автобусов).

В программном коде реализованы следующие ключевые функции:

- `poisson_probability(n, λ)` – вычисление вероятности наступления ровно n событий;

⁵³ «Правда, чистая правда и статистика» или «15 распределений вероятности на все случаи жизни» // Хабр. URL: <https://habr.com/ru/articles/311092/#Puasson> (дата обращения: 10.04.2025).

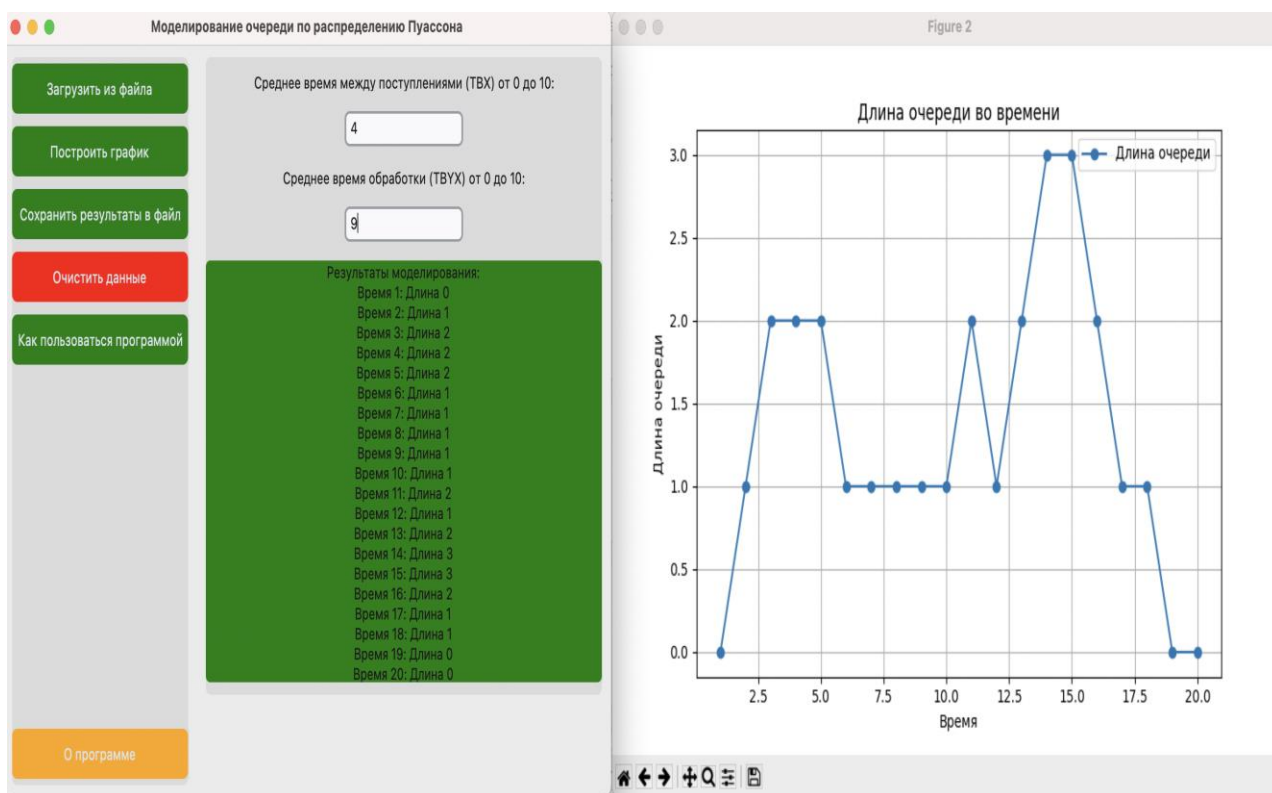
– $\text{cumulative_probability}(n, \lambda)$ – вычисление вероятности наступления не более n событий;

– $\text{simulate_queue}(\text{lambda_in}, \text{lambda_out})$ – моделирование очереди на основе введенных параметров интенсивности поступления и обслуживания.

Программа позволяет пользователю определить среднюю длину очереди, среднее время ожидания и вероятность простоя обслуживающего элемента. При помощи графиков можно отследить развитие очереди в динамике.

Юридический статус и значимость.

Программный код был подан на государственную регистрацию в качестве ЭВМ и получил регистрационный номер, подтверждающий авторство и юридическую защиту.



Таким образом, программа представляет собой инструмент анализа эффективности системы обслуживания. Она позволяет моделировать влияние изменения параметров, что способствует обоснованию управленческих решений (например, необходимости увеличения числа сотрудников или оптимизации расписания). Разработанная программа может использоваться в учебных и исследовательских целях, а также при моделировании реальных бизнес-процессов. Её преимущество заключается в простоте интерфейса и адаптивности под различные сценарии. Регистрация как ЭВМ подтверждает её уникальность и авторский вклад.

Пархачёва Алина Андреевна,

обучающаяся 2 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры

информационной безопасности в управлении Удмуртского

государственного университета,

г. Ижевск

СОВРЕМЕННОЕ СОСТОЯНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В ЭЛЕКТРОЭНЕРГЕТИКЕ РАЗНЫХ СТРАН

В условиях современных технологий и увеличения зависимости от цифровых решений, киберугрозы становятся реальной проблемой для энергетической отрасли. Энергетические предприятия относятся к объектам критически важной инфраструктуры, и от их стабильной работы зависит жизнь простых граждан и нормальное функционирование крупных корпораций. По этой причине проблема информационной безопасности в энергетической отрасли в настоящее время привлекает большое внимание⁵⁴.

Наиболее уязвимыми являются страны с развивающейся экономикой, где уровень кибербезопасности нередко остается на низком уровне. Наиболее распространенными регионами, где происходят такие атаки, являются:

- Северная Америка: 35 % всех атак.
- Европа: 25 %.
- Азия: 20 %.
- Латинская Америка и Африка: оставшиеся 20 %.

Эти данные подчеркивают глобальность проблемы и необходимость международного сотрудничества в борьбе с киберугрозами.

Согласно отчету Sophos, 49 % инцидентов в энергетической сфере происходят из-за уязвимостей, 27 % – от скомпрометированных учетных данных, 14 % – из-за вредоносных писем⁵⁵.

⁵⁴ Кибербезопасность в энергетике – задача государственного уровня // InformationSecurity. URL: <https://goo.su/IM6Q> (дата обращения: 10.04.2025).

⁵⁵ Кибератаки в энергетическом секторе // INFOWATCH. URL: <https://goo.su/WPgJy> (дата обращения: 10.04.2025).

Примеры крупных атак на электроэнергетику.

1. Атаки на систему управления энергетической сетью Украины в 2015 и 2016 годах⁵⁶.

2015 год (BlackEnergy): Эта атака считается первым в истории случаем успешной кибератаки, вызвавшей отключение электроэнергии. Злоумышленники использовали вредоносное ПО BlackEnergy для проникновения в сети трех украинских энергетических компаний. Они получили удаленный доступ к системам управления (SCADA) и вручную отключили подстанции, оставив без света около 225 000 потребителей на несколько часов. Помимо отключения электроэнергии, атака включала в себя вывод из строя систем мониторинга и управления, а также уничтожение данных.

Метод: Фишинг, социальная инженерия для получения учетных данных, эксплуатация уязвимостей в VPN и SCADA-системах.

Последствия: Отключение электроэнергии, повреждение оборудования, нарушение работы систем мониторинга и управления.

2016 год (Industroyer/CrashOverride): Эта атака была еще более сложной и автоматизированной, чем атака 2015 года. Злоумышленники использовали вредоносное ПО Industroyer (также известное как CrashOverride), которое было специально разработано для поражения промышленных систем управления, используемых в электроэнергетике. Industroyer позволял управлять выключателями и другими устройствами в подстанциях, приводя к масштабным отключениям электроэнергии. Атака также включала в себя DDoS-атаки на центры обработки вызовов и уничтожение данных.

Метод: Вредоносное ПО, разработанное для управления промышленными системами управления (SCADA). Использовались различные протоколы, применяемые в электроэнергетике (IEC 60870-5-101, IEC 60870-5-104, IEC 61850).

Последствия: Отключение электроэнергии, повреждение оборудования, нарушение работы систем мониторинга и управления.

2. Атака на Colonial Pipeline в США в 2021 году⁵⁷.

В начале мая крупнейший в США трубопровод Colonial Pipeline стал жертвой шифровальщика DarkSide. В результате сеть компании была зашифрована, а преступники стали обладателями большого массива данных. Colonial Pipeline была вынуждена приостановить работу топливопровода.

⁵⁶ Подробности о беспрецедентном взломе электрической сети Украины // Хабр. URL: <https://goo.su/nsycXRm> (дата обращения: 11.04.2025).

⁵⁷ Темные хроники: к чему привела атака на Colonial Pipeline // Kaspersky ICS CERT. URL: <https://goo.su/ZWDuq> (дата обращения: 11.04.2025).

Спустя два дня после атаки власти объявили чрезвычайное положение в 17 штатах и округе Колумбия. Часть АЗС были временно закрыты, а средняя по стране цена галлона бензина поднялась до рекордных значений за последние 7 лет. Из-за нехватки топлива авиакомпания American Airlines была вынуждена изменить некоторые рейсы. За дешифровку компания заплатила выкуп в размере 4,4 млн долл. США.

DarkSide действовали по схеме Ransomware-as-a-Service (RaaS), когда авторы шифровальщика поддерживают и развивают вредоносное ПО, инфраструктуру для партнеров, кошельки для получения выкупа и т.д., предоставляют средства для переговоров с компанией-жертвой (и, при необходимости, берут такие переговоры на себя), а «внешние» операторы используют зловред в атаках на скомпрометированные ими системы. В случае успеха деньги потом делятся в заранее оговоренных долях.

3. Атака на K-Electric в 2019 году⁵⁸.

В сентябре 2019 года компания K-Electric, крупнейший поставщик электроэнергии в Карачи (крупнейший город Пакистана), подверглась серьезной кибератаке, которая привела к сбоям в работе ее IT-систем и веб-сайта. Атака была осуществлена с использованием вымогательского ПО (ransomware), предположительно MegaCortex.

Последствия:

1) Нарушение работы IT-систем: атака зашифровала важные данные и нарушила работу IT-систем компании, включая биллинговые системы, системы обслуживания клиентов и веб-сайт.

2) Затруднения для клиентов: клиенты K-Electric испытывали трудности с оплатой счетов, получением информации и сообщением об авариях.

3) Отсутствие отключений электроэнергии (важный момент): важно отметить, что атака не привела к отключениям электроэнергии в Карачи. Злоумышленники не смогли проникнуть в системы управления электроснабжением.

4. Атака на систему управления энергетической сетью в Венесуэле в 2019 году⁵⁹.

В марте 2019 года Венесуэла столкнулась с масштабным отключением электроэнергии, которое затронуло большую часть страны на несколько дней. Правительство Венесуэлы заявило, что причиной отключения стала кибератака

⁵⁸ Шифровальщик Netwalker атаковал одного из крупнейших поставщиков электроэнергии в Пакистане // Хакер. URL: <https://goo.su/ikAHv> (дата обращения: 11.04.2025).

⁵⁹ Атака на систему энергоснабжения Венесуэлы велась из двух городов США // RGRU. URL: <https://goo.su/scKS> (дата обращения: 11.04.2025).

на систему управления гидроэлектростанцией им. Симона Боливара. По версии правительства, атака была направлена на нарушение работы SCADA-систем и привела к сбою в работе станции.

Последствия:

1) Остановка производства: многие предприятия и производства были вынуждены приостановить свою деятельность.

2) Проблемы с водоснабжением: отключение электроэнергии привело к перебоям в водоснабжении.

3) Сбои в работе больниц и других критически важных объектов: больницы, школы и другие критически важные объекты испытывали трудности из-за отсутствия электроэнергии.

4) Социальные протесты и беспорядки: отключение электроэнергии вызвало социальные протесты и беспорядки.

Методы предотвращения кибератак⁶⁰

1. Мониторинг и анализ сетевого трафика:

Используйте мониторинг трафика для выявления подозрительной активности, анализируйте логи систем для поиска аномалий и применяйте инструменты обнаружения аномалий для быстрого выявления кибератак.

2. Многофакторная аутентификация:

Внедрите многофакторную аутентификацию, требующую дополнительное подтверждение личности (код из SMS, биометрия).

3. Регулярные аудиты и тестирование уязвимостей:

Проводите регулярные аудиты систем и сетевых устройств для выявления уязвимостей. Используйте тестирование уязвимостей (симуляцию атак) и специализированные инструменты для обнаружения слабых мест. Технические средства должны быть подкреплены организационными мерами, такими как создание специальных команд по кибербезопасности и установление четких протоколов реагирования на инциденты.

Программы обучения и повышения осведомленности сотрудников⁶¹

Обучение персонала – основа кибербезопасности. Каждый сотрудник – часть системы защиты.

1. Защита от фишинга и социальной инженерии:

Необходимо обучать сотрудников распознавать подозрительные сообщения и ссылки, выявлять поддельные сайты, использовать надежные пароли и двухфакторную аутентификацию. Важно научить безопасному поведению в сети.

⁶⁰ Защита от блэкаутов и катастроф – информационная безопасность в электроэнергетике // CISCOLAB. URL: <https://goo.su/pLLna> (дата обращения: 11.04.2025).

⁶¹ Кибербезопасность электроэнергетической инфраструктуры // kaspersky. URL: <https://goo.su/15JEG> (дата обращения: 12.04.2025).

5. Примеры программ обучения:

Компании используют онлайн-тренинги, симуляции атак для практики, и регулярные семинары для обновления знаний.

6. Важность обучения:

Обучение повышает осведомленность и помогает предотвратить атаки. Обученные сотрудники быстрее реагируют на инциденты и минимизируют ущерб. Хорошо обученный персонал – первая линия обороны.

Таким образом, поддержание высокого уровня кибербезопасности в энергетической отрасли – это неразрывная часть обеспечения национальной безопасности. Призываю всех к совместным усилиям для защиты нашей критической инфраструктуры от кибератак.

Поносова Анастасия Денисовна,

Рахимов Ильтан Эльмирович,

*обучающиеся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».*

*Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры
информационной безопасности в управлении Удмуртского
государственного университета,
г. Ижевск*

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ЦЕПЯМ ЭЛЕКТРОПИТАНИЯ

Современные электронные и информационные системы функционируют в условиях постоянно возрастающих угроз утечки конфиденциальной информации. При этом особую обеспокоенность вызывают технические каналы утечки, не зависящие от логической или сетевой структуры систем. Одним из таких каналов, часто упускаемым из внимания, являются цепи электропитания, которые при определённых условиях становятся проводниками несанкционированного распространения информационных сигналов.

- На практике это означает, что сигналы, отражающие логику работы оборудования, могут непреднамеренно передаваться по силовым цепям и восприниматься за пределами контролируемой зоны. Подобные явления порождают необходимость в глубоком понимании механизмов утечки и реализации комплекса защитных мер. В настоящей статье проведён системный анализ

таких угроз, рассмотрены основные каналы утечки и предложены эффективные подходы к их минимизации⁶².

1. Механизмы утечки информации по цепям электропитания.

1.1. Гальваническая связь.

Гальваническая связь возникает в тех случаях, когда две или более цепи имеют общее сопротивление в контуре возврата тока. Это может быть общий провод питания, заземления или сопротивление на участке шинпровода. В такой конфигурации ток одного устройства индуцирует паразитное напряжение в другом:

$$u(t) = R \cdot i(t) + L \cdot (di/dt)$$

Даже при минимальном уровне тока сигналы могут быть достаточно отчётливыми, чтобы их можно было выделить и интерпретировать, особенно при наличии чувствительных усилительных каскадов.

1.2. Паразитные емкости и индуктивности.

Каждый электрический проводник обладает неидеальными характеристиками: паразитной ёмкостью и индуктивностью. На высоких частотах эти элементы играют значимую роль в передаче сигнала. Ёмкостные и индуктивные связи между соседними проводами могут выступать в качестве несанкционированных каналов утечки. Эффект особенно ярко выражен:

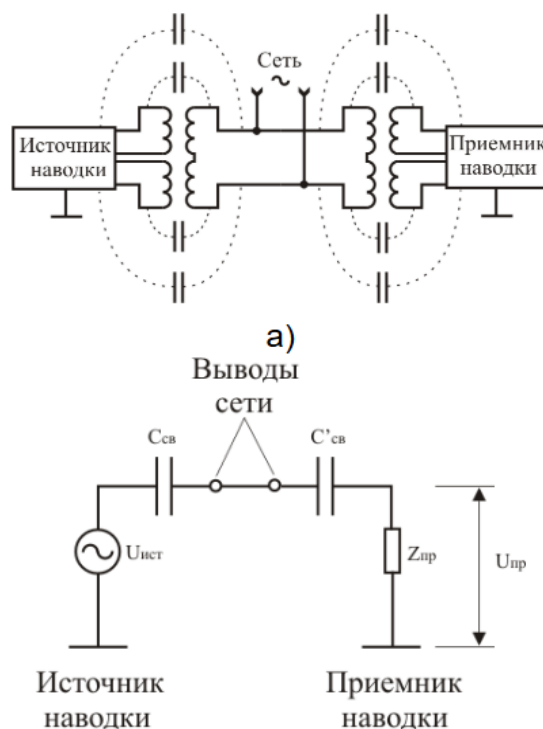
- при наличии длинных или параллельных трасс;
- в условиях высокой плотности монтажа;
- при недостаточной экранированной защите;
- при отсутствии развязки по питанию⁶³.

1.3. Асимметричные наводки.

На практике значительная часть нежелательных наводок между удаленными друг от друга устройствами происходит с участием сети питания. При этом возможны различные ситуации. В случае асимметричной наводки, когда провода сети питания прокладываются вместе и имеют одинаковые емкости относительно источников и приемников наводки, в них наводятся напряжения, одинаковые по величине и по фазе относительно земли и корпуса приборов. На рис. 1 представлены действительная и эквивалентная схемы нежелательной асимметричной связи двух устройств, питающихся от общей сети.

⁶² ГОСТ Р 51275-99. Защита информации. Объект информатизации. Общие положения. URL: <https://internet-law.ru/gosts/gost/8680/>

⁶³ Противодействие экономическому шпионажу : сборник статей журнала “Защита информации. Конфидент”. Санкт-Петербург : Конфидент, 2000. URL: <https://dvboyarkin.ru/wp-content/uploads/2019/11/uchebnik-TZI.pdf>



Это приводит к тому, что разность потенциалов между проводами становится информативной и поддается анализу.

1.4. Побочные электромагнитные излучения (ПЭМИН).

Электронные устройства, особенно с импульсным питанием или высокой частотой переключений, неизбежно создают электромагнитные поля. Провода питания, особенно неэкранированные и с большим распространением, действуют как антенны – они не только воспринимают внешние поля, но и излучают внутренние сигналы наружу. В этом случае возможна утечка информации даже без физического подключения к цепи питания.

1.5. Вторичные источники питания.

Источники питания нередко выступают не как барьеры, а как проводники утечки. Если усиленные сигналы в функциональных блоках замыкаются на землю через внутренние элементы питания, то на этих элементах формируется напряжение, которое отражает форму обрабатываемого сигнала. При слабой фильтрации это напряжение попадает в питающую линию и уходит за пределы защищаемого пространства.

1.6. Недостатки трансформаторной развязки.

Трансформаторы, применяемые для развязки, обеспечивают хорошую фильтрацию на низких частотах, но в условиях ВЧ-воздействий могут не обеспечивать должного затухания. В результате высокочастотные компоненты сигнала передаются с первичной обмотки на вторичную, нарушая изоляцию и создавая новый канал для утечки⁶⁴.

⁶⁴ Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. Москва : Гротек, 1997. URL: <https://www.dissercat.com/content/ekonomicheskie-osnovy-teorii-proektirovaniya-sistem-zashchity-informatsii>

2. Последствия утечки информации.

Потенциальные риски при реализации описанных механизмов включают:

- Компрометацию конфиденциальной информации – вплоть до восстановления обрабатываемых данных на основе анализа наводок.
- Нарушение целостности системы – внедрение управляющих сигналов через обратные каналы питания или создания помех.
- Распространение вредоносного кода – при наличии уязвимостей в импульсных преобразователях возможно внедрение сигнала через силовые цепи.

3. Методы защиты от утечки информации.

3.1. Технические меры.

- Применение сетевых фильтров, LC-цепей, ферритов и стабилизаторов.
- Использование экранированных кабелей с двойным заземлением.
- Разделение цепей питания по зонам секретности.
- Введение изоляции по трансформаторам с усиленной развязкой.
- Установка фильтров ПЭМИН на все внешние линии.

3.2. Архитектурные решения.

- Формирование контролируемой зоны в пределах объекта.
- Устройство помехозащищённых помещений с экранированными стенами.
- Прокладка силовых и информационных линий в разнесённых трассах.
- Применение antivибрационных вставок и демпфирующих материалов в трубопроводах и коммуникациях.

3.3. Организационные меры.

- Ведение учета каналов утечки и слабых мест системы.
- Создание режимных зон и разграничение полномочий доступа.
- Проведение аттестации и аудита объектов защиты.
- Установление матрицы доступа к конфиденциальной информации.

4. Регламент и нормативные требования.

Организация защиты информации от утечки по цепям электропитания осуществляется в соответствии с рядом нормативных документов, в том числе:

- Конституцией Российской Федерации.
- Федеральными законами «О государственной тайне», «О коммерческой тайне», «Об информации».
- ГОСТ Р 51275-99.
- Положениями ФСТЭК и ФСБ России по СТЗИ.
- Методическими рекомендациями по проектированию и аттестации защищаемых объектов.

Создание СТЗИ требует проведения обследований, проектирования, внедрения технических средств, а также документальной аттестации соответствия⁶⁵.

⁶⁵ *Торокин А.А.* Инженерно-техническая защита информации. Москва : Гелиос АРВ, 2005. URL: <https://studfile.net/preview/5815465/>

Пославская Виктория Яновна,

слушатель 5 курса Радиотехнического факультета

Воронежского института МВД России.

Научный руководитель: А.А. Терентьев, к.т.н., старший преподаватель

Воронежского института МВД России,

г. Воронеж

АВТОМАТИЗАЦИЯ ПРОЦЕДУРЫ ОБРАБОТКИ ЭКСПЕРТНЫХ РЕШЕНИЙ В ОВД

Моделирование является мощным и широко распространенным методом исследования систем и явлений, используемым практически во всех отраслях науки и техники. Применение информационных технологий, построенных на основе математических моделей и алгоритмов, позволит автоматизировать процесс обработки экспертных оценок, что повлечет за собой ускорение процесса выбора необходимых технических средств для нужд МВД России⁶⁶.

Основная цель работы – это автоматизация процесса экспертного опроса в органах внутренних дел. Яркий пример такого рода деятельности, это сравнение экспертами различных образцов оборудования для выбора, наиболее подходящего с целью последующей закупки и использовании практической деятельности.

Для его наиболее эффективного подбора привлекаются силы экспертов, осуществляющих сравнение и анализ имеющихся на рынке образцов для последующего выбора наиболее подходящих в интересах МВД России.

С целью автоматизации было разработано программное обеспечение⁶⁷, решающие все вышеперечисленные задачи по осуществлению экспертных опросов, так как именно за счёт них может осуществляться принятие самых разных решений, начиная от выбора технических средств для нужд органов внутренних дел, как было сказано выше, так и принятие абсолютно любых коллегиальных решений с учётом мнений всех респондентов.

⁶⁶ О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы : Указ Президента РФ от 9 мая 2017 г. № 203 : [Электронный ресурс]. Режим доступа: <https://base.garant.ru/71670570/> (дата обращения: 17.11.2023).

⁶⁷ Бакулин Н.С., Терентьев А.А. Автоматизированный программный комплекс распределённой экспертной оценки // Свидетельство о регистрации программы для ЭВМ № 2024660433. URL: <https://www.elibrary.ru/item.asp?id=67264132> (дата обращения: 30.03.2025).

Суть ранее разработанного метода^{68,69} заключается в следующем, у нас имеется перечень объектов, которые мы будем сравнивать для получения наиболее подходящего нам объекта. Для этого составляется матрица $A [n * n]$, данная матрица разбивается на m slice-матриц. Используя фундаментальную шкалу МАИ, происходит заполнение slice-матриц V_i . При этом результаты попарного сравнения с эталонным объектом размещаются в первой строке матрицы. Проверяется согласованность slice-матриц с помощью вычисления индекса согласованности S_{aati} ^{70,71}. Если индекс согласованности неудовлетворителен, матрица предоставляется эксперту для повторного заполнения.

«DAS» (Distributed Assessment System) – распределённая система оценок, предназначен для организации и осуществления автоматизированной распределённой экспертной оценки попарно сравниваемых объектов. Программный комплекс разработан на языке C++ с использованием библиотеки «Qt» с открытым исходным кодом.

Qt позволяет запускать написанное с его помощью программное обеспечение в большинстве современных операционных систем путём простой компиляции программы для каждой системы без изменения исходного кода (что позволяет без затруднений адаптировать программный продукт для использования в ОС Astra Linux).

Разработанный программный комплекс реализован на базе клиент серверной архитектуры используя протокол TCP. Данная реализация обеспечивает централизованную обработку полученных от экспертов данных, а «лёгкие» клиентские приложения выступают лишь в роли внешних интерфейсов для корректного и удобного сбора данных, что минимизирует вычислительную нагрузку на ЭВМ экспертов.

Данный программный комплекс организуется по топологии «звезда», где в роли центрального элемента выступает программа – сервер, обрабатывающая всю информацию, поступающую с периферийных программ – клиентов.

⁶⁸ Пьянков О.В., Терентьев А.А. Разработка численного метода определения весов конфликтных взаимодействий // Вестник Воронежского института МВД России. 2019. № 1. С. 69–74.

⁶⁹ Терентьев А.А. Моделирование и параметрическая оптимизация проведения экспертного опроса с помощью slice-матриц // Вестник Воронежского государственного университета. 2020. № 2. С. 127–135.

⁷⁰ Саати Т.Л. Принятие решений при зависимостях и обратных связях: Аналитические сети / пер. с англ. ; науч. ред. А.В. Андрейчиков, О.Н. Андрейчикова. Изд. 3-е. Москва : ЛИБРОКОМ, 2011. 360 с.

⁷¹ Саати Т.Л. Принятие решений. Метод анализа иерархий / пер. с англ. Р.Г. Вачнадзе. Москва : Радио и связь, 1993. 278 с.

Данный программный комплекс реализован на концепции объектно ориентированного программирования. Клиентское приложение, выступающее в роли внешнего интерфейса, и имеет в своём составе лишь два модуля.

- модуль ТСП клиента;
- модуль отображения.

Модуль ТСП клиента обеспечивает обмен данными и внутренними командами с приложением – сервером.

Модуль отображения реализует удобную визуализацию полученных данных, их корректное отображение и удобный ввод для последующей отправки.

Серверное приложение имеет более сложную структуру за счёт того, что сама организация экспертной оценки, математическая обработка результатов предоставленных экспертами, формирование отчётов для последующего использования или более детального анализа результатов экспертной оценки возлагается именно на него, и состоит из ряда модулей (рис. 1).

ТСП сервер является ядром серверного приложения и отвечает за передачу данных и служебных команд между сервером и клиентами.

Модуль контроля учётных записей отвечает за администрирование учётных записей пользователей и их авторизацию. В функционал данного модуля входит создание новых учётных записей с возможностью автоматической генерации учётных данных, удаление уже имеющихся учётных записей, отображение все зарегистрированных учётных записей с отслеживанием статуса их подключения, выгрузка учётных данных для предоставления их пользователям – экспертам.

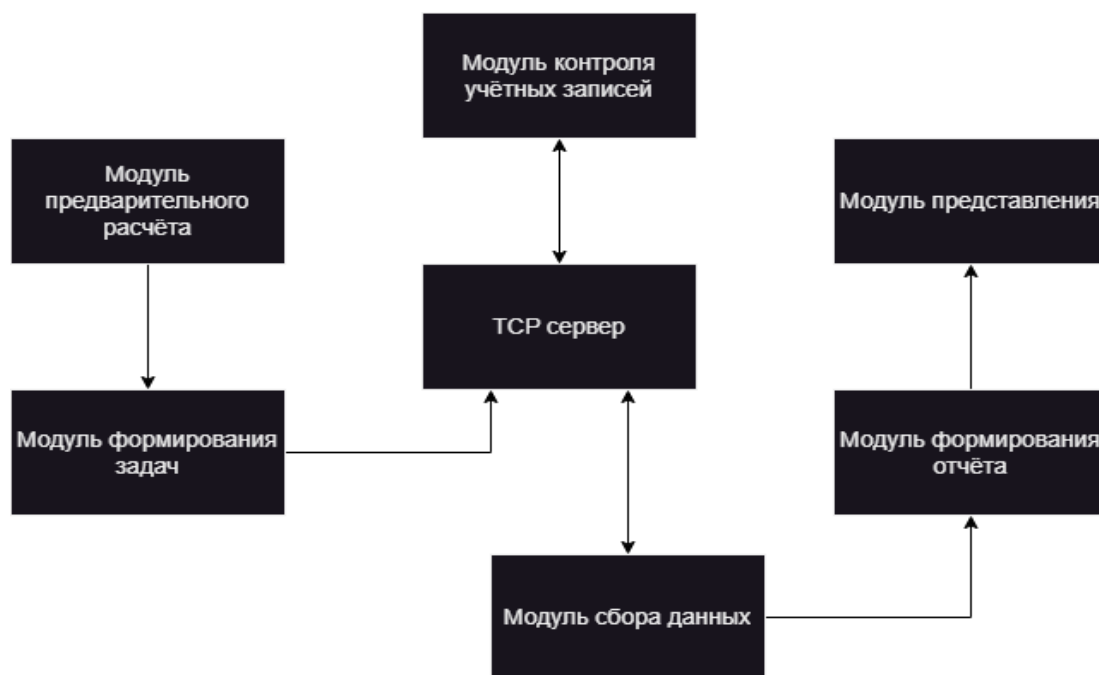


Рис. 1. Архитектура серверного программного обеспечения.

Модуль предварительного расчёта отвечает за расчёт количества экспертов, требуемых для экспертной оценки, данный модуль реализует подсчёт необходимого количества экспертов исходя из вышеописанной математической модели, так же обеспечивает ввод данных о сравниваемых объектах.

Модуль формирования задач подготавливает пакеты данных исходя из указанных администратором (пользователем серверного приложения) для каждого эксперта и передаёт на ТСР сервер для отправки.

Модуль сбора данных получает данные от экспертов и осуществляет их предварительную обработку, предварительно размещая данные в контейнеры для последующей математической обработки и отображения.

Модуль формирования отчёта производит математическую обработку полученных от экспертов данных согласно описанной выше математической модели, а именно рассчитывает векторы приоритетов, производит их нормировку.

Модуль представления осуществляет удобное для пользователя представление данных рассчитанных предыдущем модулем, обеспечивает визуализацию собранных данных путём построения графика, обеспечивает обзор не только общего итогового отчёта, но и отчётов каждого из экспертов фиксируя как их экспертные оценки, так и время, затраченное ими на работу, позволяет выгрузить отчёт из программы для его последующего использования или более детального анализа.

Разработанный программный комплекс осуществляет выполнение задачи по автоматизации процесса экспертной оценки в полной мере, имеет широкий функционал, а за счёт использования объектно ориентированного языка программирования C++ в тандеме с библиотекой Qt позволяет проводить экспертную оценку объектов, минимизируя зависимости от скорости передачи данных внутри локальной сети и вычислительных мощностей ЭВМ.

Описанный программный комплекс прошел стадию апробирования, результаты проведения данного эксперимента приведены в работе⁷².

⁷² Терентьев А.А., Бакулин Н.С. Результаты апробации программного комплекса «DAS» // Общественная безопасность, законность и правопорядок в III тысячелетии. 2024. № 10-2. С. 138-142.

Пославская Виктория Яновна,

слушатель 5 курса Радиотехнического факультета

Воронежского института МВД России.

Научный руководитель: А.А. Терентьев, к.т.н., старший преподаватель

Воронежского института МВД России,

г. Воронеж

ПРОЕКТИРОВАНИЕ СЕГМЕНТА СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ДЛЯ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

На этапе развития технологий и информационных систем ставится вопрос о правильном обеспечении безопасности данных и различных систем. Одним из способов обеспечивающий защиту в данном случае, является организация сетей связи специального назначения (далее СС СН). Оно исследует уникальные аспекты их планирования и функционирования, которые включают в себя шифрование данных, создание резервных каналов, защиту от различного рода атак и управление доступом.

Сети связи представляют собой технологические системы, включающие различные средства и линии связи и предназначенные для электросвязи или почтовой связи⁷³.

Что касается СС СН они разрабатываются для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка.

Типология сетей связи делится на первичные и вторичные сети. Первичная (транспортная) сеть связи включает в себя совокупность технических средств, комплексов, линий связи и обслуживающего персонала. Она предназначена для предоставления потребителям стандартных каналов (трактов) передачи первичных электрических сигналов. Основной сервис для абонентов – это типовые каналы и тракты⁷⁴.

⁷³ Курицын С.А. Телекоммуникационные технологии и системы : учеб. пособие для студ. высш. учеб. Заведений. Москва : Академия, 2008. С. 123-125.

⁷⁴ Терентьев А.А. Математическая модель аналитической деятельности ситуационных центров органов внутренних дел // Вестник Воронежского института ФСИН России. 2020. № 3. С. 92–95.

Вторичная сеть связи, также известная как сеть абонентского доступа, состоит из совокупности технических средств и связей, обеспечивающих потребителей разнообразными услугами по доставке, хранению и обработке информации. Основные услуги для абонентов вторичных сетей связаны с информационным обменом.

Задача сети связи специального назначения заключается в доставке информации между распределенными в пространстве органами и пунктами системы управления, обслуживающими органы государственной власти, обороны, безопасности и правопорядка.

Следует учесть, что такие сети отличаются высокой степенью защищенности, адаптивностью и возможностью функционирования в условиях препятствий и ограничений. Однако в определенных случаях (примером может послужить то, что промышленным предприятиям необходимо полагаться на автоматизацию и интеллектуальных систем управления, в таком случае локальная обработка данных выступает для мониторинга и контроля производственного процесса) наиболее эффективным способом защиты безопасности служат локализованные решения, которые выступают в качестве локально вычислительной сети (далее ЛВС), которые обеспечивают оперативное взаимодействие между различными сегментами подобных систем.

ЛВС объединяет разнообразные вычислительные устройства в единую сеть, обеспечивая мгновенный обмен данными и доступ к необходимым ресурсам. Это позволяет более эффективно управлять ресурсами, минимизировать задержки в передаче информации и обеспечить высокий уровень безопасности.

Локально вычислительные сети могут использоваться как для конкретных задач, требующих быстрой реакции и взаимодействия между различными подразделениями, так и в качестве резервных систем связи. Они создают надежный канал передачи данных, который может функционировать независимо от внешних инфраструктур, что особенно важно в ситуациях, когда стандартные каналы могут оказаться недоступными или подверженными угрозам⁷⁵.

Внедрение ЛВС в структуры сетей связи специального назначения открывает новые возможности для стратегического планирования и оперативного управления, обеспечивая высокую степень автономности и независимости от внешних факторов. Это перспективное направление развития позволяет оптимально сочетать преимущества глобальных сетей с гибкостью и локализованной безопасностью локальных решений, обеспечивая надежную и эффективную связь в любых условиях.

⁷⁵ *Асратян Р.Э., Лебедев В.Н.* Распределенные аналитические системы на основе средств информационного взаимодействия в гетерогенной глобально-сетевой среде. Москва : ЛЕНАНД, 2010. С. 34-37.

Специальные сети связи и локальные вычислительные сети (ЛВС) играют особую роль в этой динамичной среде, обеспечивая надежную, безопасную и оперативную передачу данных. Эти сети часто служат основой для мультифункциональных систем управления, связи и обмена информацией, критически важных для выполнения задач различной сложности и значимости.

Построение структурной схемы таких сетей является важным и многогранным процессом, сочетающим в себе элементы инженерии, информационной безопасности и управления проектами. Грамотное проектирование и внедрение структурной схемы позволяет гарантировать непрерывную работу систем, их устойчивость к отказам и внешним угрозам, а также возможность последующей модернизации.

Мы будем рассматривать подразделение на базе которого развертывается совокупность используемых автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, систем связи и передачи данных (рис. 1 и 2).

На рисунке 1 показана структурная схема подключения сети с выходом в ИСОД и обеспечения ЛВС с выходом в интернет⁷⁶.

На рисунке 2 показана развернутая сеть подразделения двух этажей, подразумевая, что остальные этажи будут обеспечиваться защищенной сетью по аналогии.

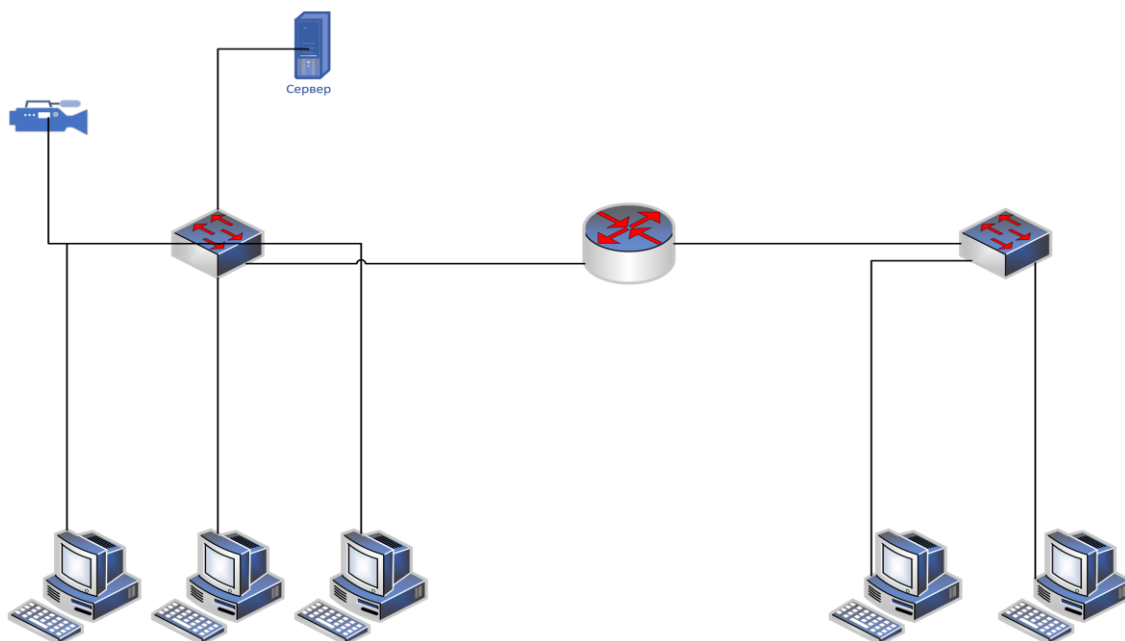


Рис. 1. Структурная схема сегмента сети специальной связи.

⁷⁶ Монахов М.Ю. Математическая модель аналитической деятельности администратора безопасности информационно-телекоммуникационной системы // Динамика сложных систем. Москва, 2015. С. 13–15.

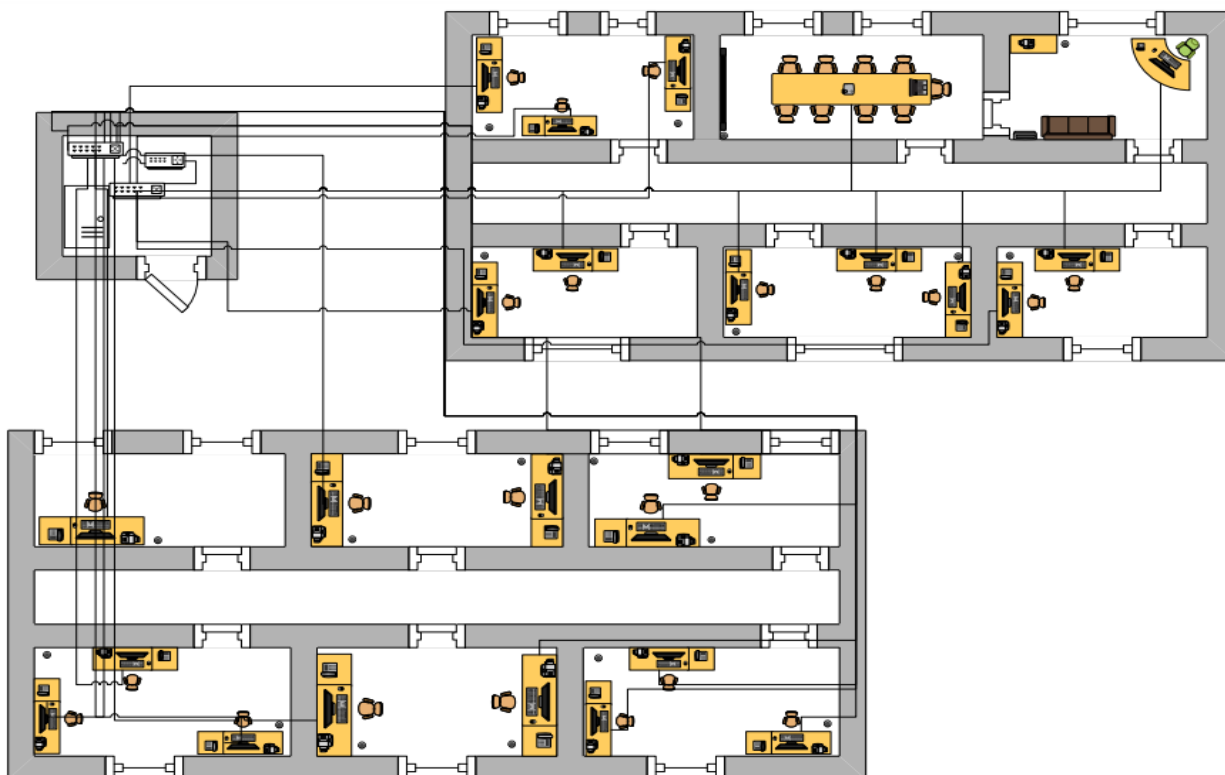


Рис. 2. Поэтажная план схема организации сети специальной связи.

Построение структурной схемы таких сетей является важным и многогранным процессом, сочетающим в себе элементы инженерии, информационной безопасности и управления проектами⁷⁷. Грамотное проектирование и внедрение структурной схемы позволяет гарантировать непрерывную работу систем, их устойчивость к отказам и внешним угрозам, а также возможность последующей модернизации.

⁷⁷ Терентьев А.А. Модели аналитической деятельности ситуационных центров органов внутренних дел // Охрана, безопасность, связь – 2020 : сб. науч. тр. Международной научно-практической конференции. Ч. 5-3. Воронеж, 2020. С. 21–24.

Потемкина Татьяна Михайловна,

обучающаяся 4 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: О.В. Меркушев, к.т.н., доцент кафедры

информационной безопасности в управлении Удмуртского

государственного университета,

г. Ижевск

ТРЕБОВАНИЯ, РЕГЛАМЕНТИРУЮЩИЕ ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

В современном мире, характеризующемся бурным развитием цифровых технологий и всеобщей цифровизацией, организации сталкиваются с постоянно растущей угрозой компрометации информации. Эта угроза затрагивает три фундаментальных свойства информации: конфиденциальность (защита от несанкционированного доступа), целостность (защита от несанкционированного изменения) и доступность (гарантия своевременного доступа для авторизованных пользователей). Обеспечение безопасности информационных систем в этих условиях становится критически важным, а эффективность управления уязвимостями выступает одним из ключевых факторов, определяющих уровень защищенности⁷⁸. Уязвимость, согласно ГОСТ Р 50922-2006⁷⁹, представляет собой слабое место в информационной системе, которое может быть использовано злоумышленниками для реализации угроз безопасности данных. Эти "слабые звенья" – это бреши в программном обеспечении, ошибки в конфигурации оборудования, упущения в политиках безопасности и многое другое. Злоумышленники активно используют выявленные уязвимости для проведения различных атак, начиная от кражи конфиденциальной информации и заканчивая полным выводом из строя информационной системы организации. Последствия таких атак могут быть катастрофическими, включая финансовые потери, репутационный ущерб и даже угрозу национальной безопасности.

⁷⁸ Сдобникова И. Управление уязвимостями в 2025 году: процесс, платформы, лучшие практики // Анализ технологий. Аналитика. Anti-Malware : электрон. версия. 2025. URL: Как эффективно выстроить процесс управления уязвимостями: кейсы, практики, платформы (дата обращения: 31.03.2025).

⁷⁹ ГОСТ Р 50922-2006. Защита информации. Основные термины и определения : нац. Стандарт Российской Федерации : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 № 373-ст : введен впервые : дата введения 2008-02-01 // Кодекс : электрон. фонд правовой и нормативно.-техн. информ. URL: ГОСТ-Р-50922-2006.pdf - Яндекс Документы (дата обращения: 01.04.2025).

Для предприятий, особенно тех, которые относятся к критической информационной инфраструктуре (далее по тексту – КИИ), такие как энергетика, транспорт, здравоохранение и так далее⁸⁰, внедрение и поддержание эффективного процесса управления уязвимостями – это не просто желательная мера предосторожности, а обязательное требование законодательства. В России данная необходимость прямо закреплена в Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и приказом ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Эти нормативные акты устанавливают строгие требования к обеспечению безопасности КИИ, включая обязательное выявление, оценку и устранение уязвимостей. Несоблюдение этих требований влечет за собой серьезные административные и финансовые санкции.

Более того, необходимость управления уязвимостями отражена во множестве других стандартов и нормативных документов. Например, стандарт Банка России СТО БР ИББС-1.0-2014⁸¹, устанавливающий общие положения по информационной безопасности в банковской сфере, недвусмысленно указывает на необходимость управления уязвимостями как на один из ключевых элементов обеспечения безопасности. ГОСТ Р ИСО/МЭК 27002-2021⁸², представляющий собой свод лучших практик в области информационной безопасности, также содержит подробные рекомендации по выявлению, оценке и устранению уязвимостей, описывая различные методы и средства их реализации. Этот стандарт представляет собой всеобъемлющий документ, охватывающий широкий спектр мер по обеспечению информационной безопасности, и управление уязвимостями занимает в нем одно из центральных мест.

⁸⁰ Царев Е.О. Критическая информационная инфраструктура 2024 год // КИИ (187-ФЗ). Статьи. RTM Group : электрон. версия. 2024. URL: Критическая информационная инфраструктура (187-ФЗ) в 2024 году. ГосСОПКА, НКЦКИ | RTM Group (дата обращения: 25.03.2025).

⁸¹ СТО БР ИББС-1.0.2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения : Стандарт Банка России : дата введения 2014-06-01 / Банк России. Изд. Официальное. Москва, 2014. 16 с.

⁸² ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности : национальный стандарт Российской Федерации : дата введения 2021-11-30 / Федеральное агентство по техническому регулированию. Изд. Официальное. Москва : Стандартинформ, 2021. 5 с.

Эффективное управление уязвимостями включает в себя несколько ключевых этапов⁸³. Это, во-первых, регулярное сканирование информационной системы на наличие уязвимостей, используя специализированные программные средства (сканеры уязвимостей), а также анализ входящей информации об уязвимостях от регуляторов, таких как ФСТЭК⁸⁴, ФСБ⁸⁵, НКЦКИ⁸⁶ и другие. Во-вторых, оценка выявленных уязвимостей по уровню критичности, что позволяет определить приоритетность их устранения. В-третьих, разработка и реализация мер по устранению уязвимостей, которые могут включать в себя обновление программного обеспечения и/или реализацию компенсирующих мер, например, изменение конфигурации оборудования, внедрение дополнительных средств защиты и разработку и внедрение более строгих политик безопасности. Наконец, необходимо регулярно мониторить эффективность принятых мер, чтобы обеспечить постоянную защищенность информационной системы от новых угроз.

Важно понимать, что управление уязвимостями – это не одноразовая процедура, а непрерывный процесс, требующий постоянного внимания и инвестиций. Организациям необходимо создавать специализированные подразделения или привлекать внешних экспертов для реализации эффективной стратегии управления уязвимостями. Только системный подход, основанный на постоянном мониторинге, своевременном реагировании на новые угрозы и постоянном совершенствовании систем защиты, позволяет обеспечить надежную защиту информационных систем от все возрастающего количества киберугроз. Необходимо также регулярно обучать персонал основам информационной безопасности и правилам работы с конфиденциальной информацией. Только комплексный подход гарантирует достижение высокого уровня защищенности.

⁸³ Руководство по организации процесса управления уязвимостями в органе (организации) : Методический документ ФСТЭК России от 17.05.2023. Текст : электронный // КонсультантПлюс : справочно-правовая система (дата обращения: 04.04.2025).

⁸⁴ Федеральная служба по техническому и экспортному контролю.

⁸⁵ Федеральная служба безопасности.

⁸⁶ Национальный координационный центр по компьютерным инцидентам.

Распутин Илья Евгеньевич,

обучающийся ФГБОУ ВО «Государственный аграрный университет Северного Зауралья».

Научные руководители: И.В. Савчук, к.т.н., доцент, доцент кафедры энергообеспечения сельского хозяйства; И.А. Щинников, преподаватель кафедры энергообеспечение сельского хозяйства ФГБОУ ВО «Государственный аграрный университет Северного Зауралья», г. Тюмень

КОМПЛЕКСНАЯ ЗАЩИТА СЕТЕЙ ЭЛЕКТРОСНАБЖЕНИЯ

Бесперебойная генерация и доставка электроэнергии потребителям является основной задачей энергетических компаний. Однако, надежность систем электроснабжения сегодня зависит не только от надежности технических средств, но и от защиты информационных систем, обеспечивающих выполнение производственного процесса.

Поэтому, в представленной работе, рассматриваются две задачи:

- разработка релейной защиты от перемежающегося однофазного замыкания на землю;
- защита информационных систем, используемых при выработке и передаче электроэнергии.

При выборе средств защиты информации для электроэнергетической отрасли требуется понимать, что основным активом является не информация, а технологический процесс. При разработке систем обеспечения информационной безопасности в электроэнергетике речь идет не о «дежурной» защите от утечек данных, а о защите от нарушения технологического процесса за счет реализации киберугроз.

В электрических сетях 10 кВ однофазные замыкания на землю являются одной из наиболее распространенных аварийных ситуаций, особенно в условиях износа оборудования, загрязнения изоляции и других неблагоприятных факторов. В связи с этим разработка эффективных методов релейной защиты, обеспечивающих надежное обнаружение и оперативное реагирование на перемежающиеся ОЗЗ, является важной задачей для повышения надежности и безопасности эксплуатации сетей 10 кВ⁸⁷.

⁸⁷ Щинников И.А. Автоматическое изменение режима работы нейтрали в электрической сети для определения места ОЗЗ // Научно-технический вестник Поволжья. 2023. № 12. С. 576-578.

В качестве решения, с использованием блоков серии БМР3-150 и возможностей гибкой логики, разработан алгоритм, позволяющий отслеживать и подсчитывать импульсы тока нулевой последовательности. Его работа основана на наличии устойчивого напряжения нулевой последовательности в разомкнутом треугольнике.

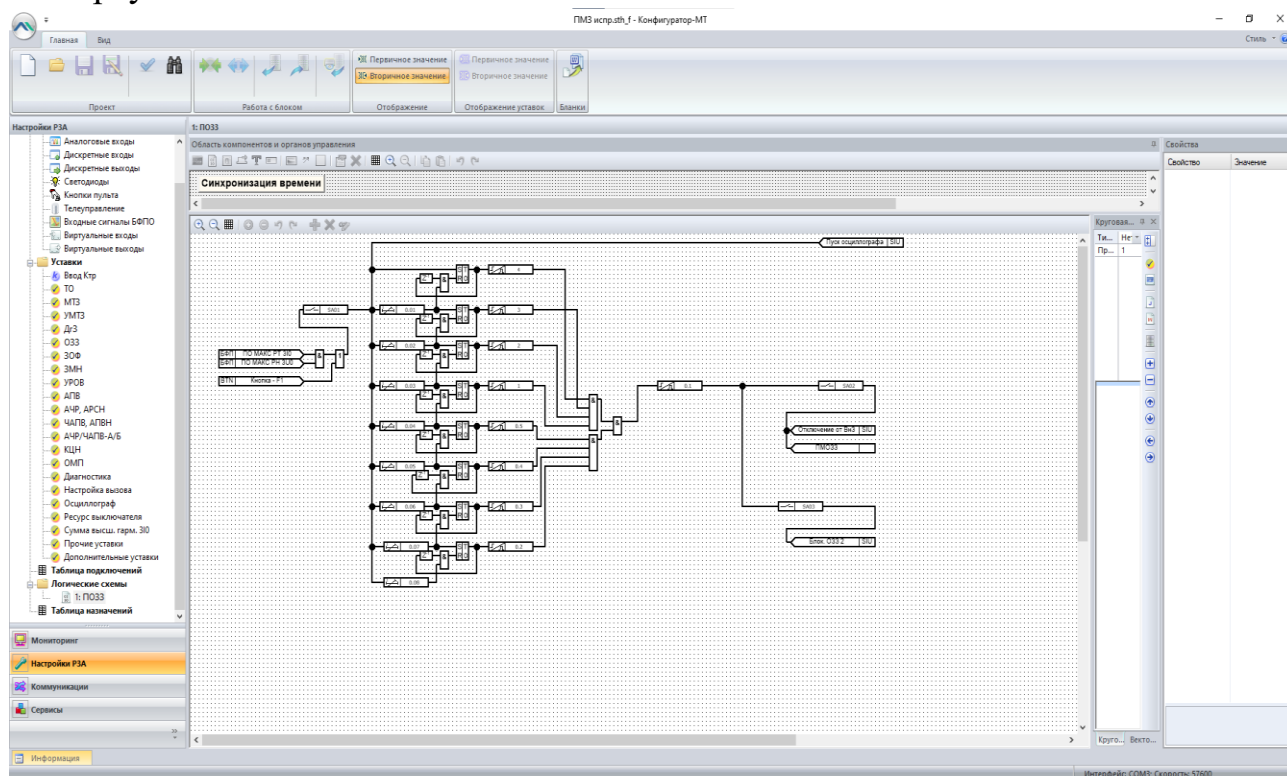


Рис. 1. Общий вид алгоритма защиты от ПМОЗЗ.

Основная концепция заключается в использовании устойчивой уставки, в большинстве случаев это $3U_0$. Когда $3U_0$ превышает установленное значение, алгоритм активируется, фиксируя импульс и удерживая его в пределах от 4 до 0,2 секунд. Важно, чтобы импульс циклически удерживался в рамках алгоритма.

После успешного удержания в цикле подается импульс ПМОЗЗ на протяжении 0,1 секунды. Далее срабатывает защита, формируя сигнал через программный ключ SA02. Одновременно через программный ключ SA03 реализуется блокировка второй ступени ОЗЗ, что приводит к отключению аварийного участка сети. (см. рисунок 1).

Разработка релейной защиты от перемежающегося однофазного замыкания на землю, обладающей способностью своевременно выявлять и оперативно реагировать на подобные замыкания, представляет собой крайне важную задачу. Она направлена на значительное повышение надежности и безопасности эксплуатации электрических сетей напряжением 10 кВ, что особенно актуально в условиях современной энергетики⁸⁸.

⁸⁸ Щинников И.А., Савчук И.В. Микропроцессорные терминалы защиты // Актуальные вопросы науки и хозяйства: новые вызовы и решения : сборник материалов ЛПМ Междуна-

Для обеспечения информационной безопасности необходимо решить следующие вопросы:

– необходима защита рабочих мест операторов и SCADA – серверов от вредоносного ПО;

– защита промышленных контроллеров от несанкционированного доступа к ним, изменения исполняемого в них кода и отправки на них некорректных команд.

Для этого необходимо предусмотреть комплексные решения по защите компонентов АСУ ТП, в том числе на базе продуктов ведущих российских разработчиков средств защиты.

Старков Василий Михайлович,

обучающийся 3 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры

информационной безопасности в управлении Удмуртского

государственного университета,

г. Ижевск

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ РАСЧЕТА ВЫПРЯМИТЕЛЯ

Разработка и совершенствование программных инструментов для автоматизации расчётов в области силовой электроники является актуальной задачей современной инженерной практики. Особый интерес представляет создание программных средств, позволяющих проводить расчёты параметров выпрямительных устройств, широко применяемых в энергоснабжении промышленных установок, системах электропривода и телекоммуникационных устройствах.

Выпрямители – это устройства, основанные на полупроводниковых компонентах (диодах, тиристорах и транзисторах), предназначенные для преобразования переменного напряжения в постоянное⁸⁹.

Расчитать выпрямитель – значит правильно подобрать диоды и определить выпрямленное напряжение. Для этого необходимо 1) знать средние значения напряжения и тока нагрузки, частоту и линейное напряжение сети;

родной студенческой научно-практической конференции, Тюмень, 29 марта 2019 года. Том Часть 2. Тюмень : Гос. аграрный университет Северного Зауралья, 2019. С. 614-616.

⁸⁹ Электрический выпрямитель // Большая российская энциклопедия. URL: <https://big-enc.ru/c/elektricheskii-vupriamitel-f9415a?ysclid=majrmlkzeb551417741> (дата обращения: 11.05.2025).

2) выбрать диоды, которые выдерживают нужные параметры; 3) рассчитать коэффициент трансформации для подбора подходящего трансформатора⁹⁰.

Целью настоящего исследования является создание учебной программы для автоматизированного расчёта параметров трёхфазного мостового выпрямителя на диодах. Реализация такой программы позволит упростить процесс расчётов, повысить точность проектирования схем и усилить практическую подготовку студентов технических специальностей.

Теоретическая значимость работы заключается в систематизации методов расчёта параметров трёхфазных выпрямителей и их алгоритмизации. Практическая значимость проявляется в разработке доступного и наглядного программного продукта для учебных целей. В настоящее время отсутствуют специализированные программные инструменты, адаптированные для образовательного использования при изучении схемотехники выпрямителей, что создаёт предпосылки для разработки новых программных решений.

Исследование проводилось в несколько последовательных этапов:

1. Анализ существующих методик расчёта параметров трёхфазного мостового выпрямителя.
2. Построение алгоритма расчёта ключевых параметров.
3. Разработка архитектуры программного обеспечения и проектирование пользовательского интерфейса.
4. Реализация программного продукта на языке Python.

В качестве базовой схемы исследования была выбрана классическая топология трёхфазного мостового выпрямителя на диодах⁹¹. Вводными параметрами служат: среднее напряжение нагрузки ($U_{но}$), средний ток нагрузки ($I_{но}$), линейное напряжение сети (U_c), частота сети (f).

На основе этих данных программа вычисляет следующие характеристики: максимальный выпрямленный ток (i), амплитуду фазного напряжения ($U_{ам}$), максимальное обратное напряжение на диодах ($U_{обр}$), коэффициент трансформации (K), мощность трансформатора (P)⁹².

Главный экран программы выполнен в минималистичном стиле, предоставляя пользователю доступ к основным функциям (см. рис. 1). Начать – переход к главному функционалу программы: вводу данных и расчётам. Метод расчётов – раздел, в котором пользователь может ознакомиться с используемыми

⁹⁰ Борисов П.А., Томасов В.С. Расчет и моделирование выпрямителей : учебное пособие по курсу “Элементы систем автоматики” (Часть I). Санкт-Петербург : СПб ГУ ИТМО, 2009. С. 4.

⁹¹ Исследование трехфазных нерегулируемых выпрямителей // Файловый архив студентов. URL: <https://studfile.net/preview/6761004/> (дата обращения: 11.05.2025).

⁹² Расчет трехфазного выпрямителя // Файловый архив студентов. URL: <https://studfile.net/preview/7724906/page:6/> (дата обращения: 11.05.2025).

формулами и методикой расчёта параметров выпрямителя. О разработчике – краткая информация об авторе проекта. *Выйти из программы* – завершение работы приложения.

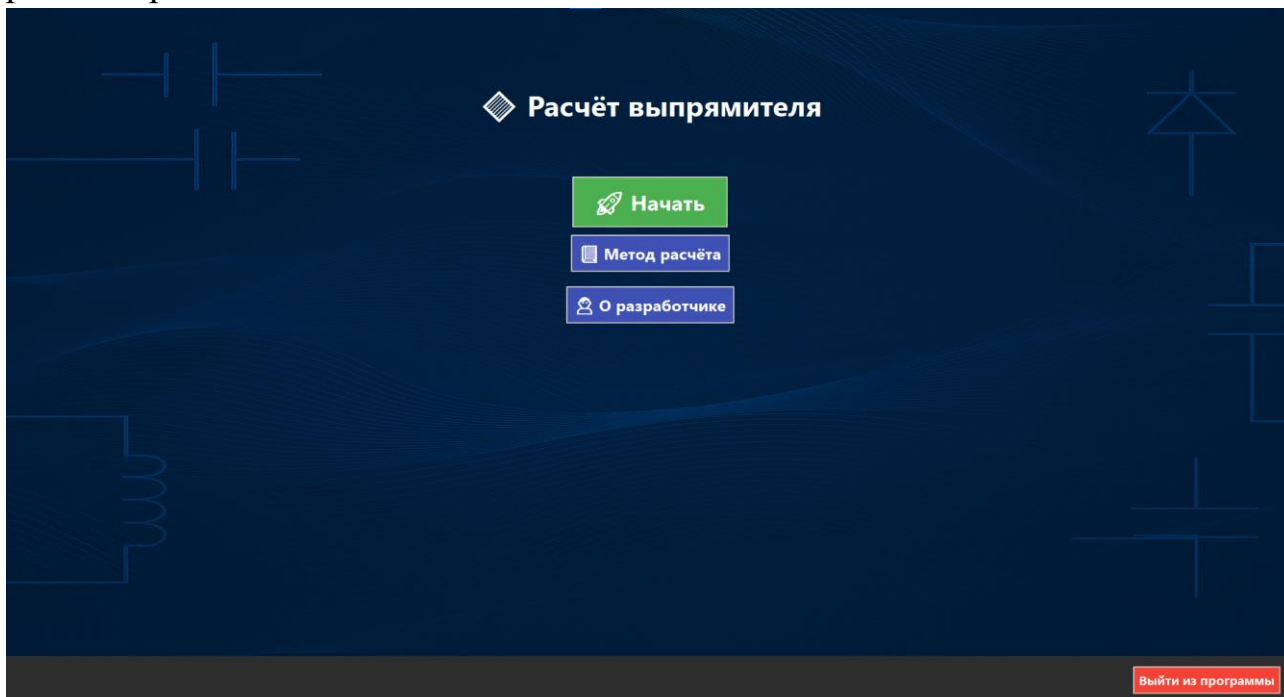


Рис. 1.

Интерфейс ввода параметров организован в виде формы с поясняющими подписями (см. рис. 2). Для повышения надёжности реализована защита от некорректного ввода: поля допускают только положительные числовые значения в установленном диапазоне. Это предотвращает ошибки на этапе задания исходных данных.

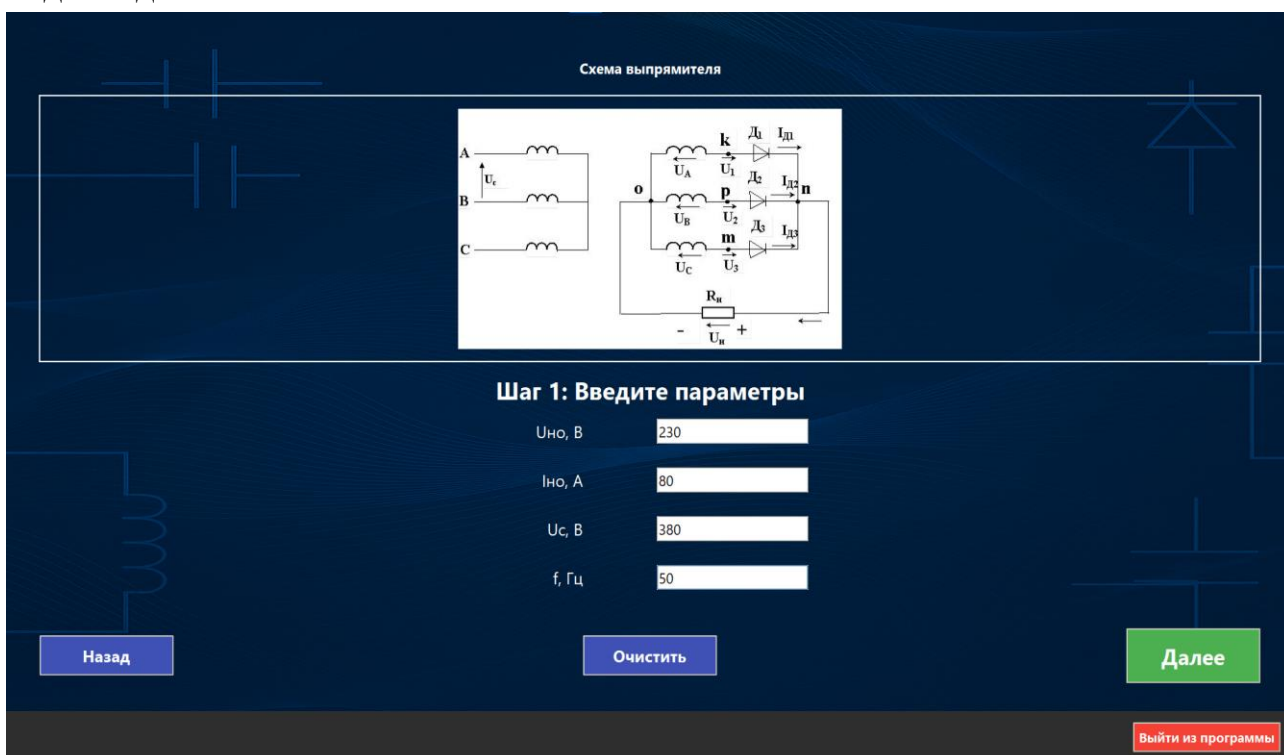


Рис. 2.

После ввода параметров программа автоматически выполняет расчёты и отображает результаты на отдельном экране (см. рис. 3). В качестве выходной информации предоставляются: значения всех рассчитанных параметров; список рекомендованных типов диодов, удовлетворяющих условиям по току и обратному напряжению; график формы выпрямленного напряжения.

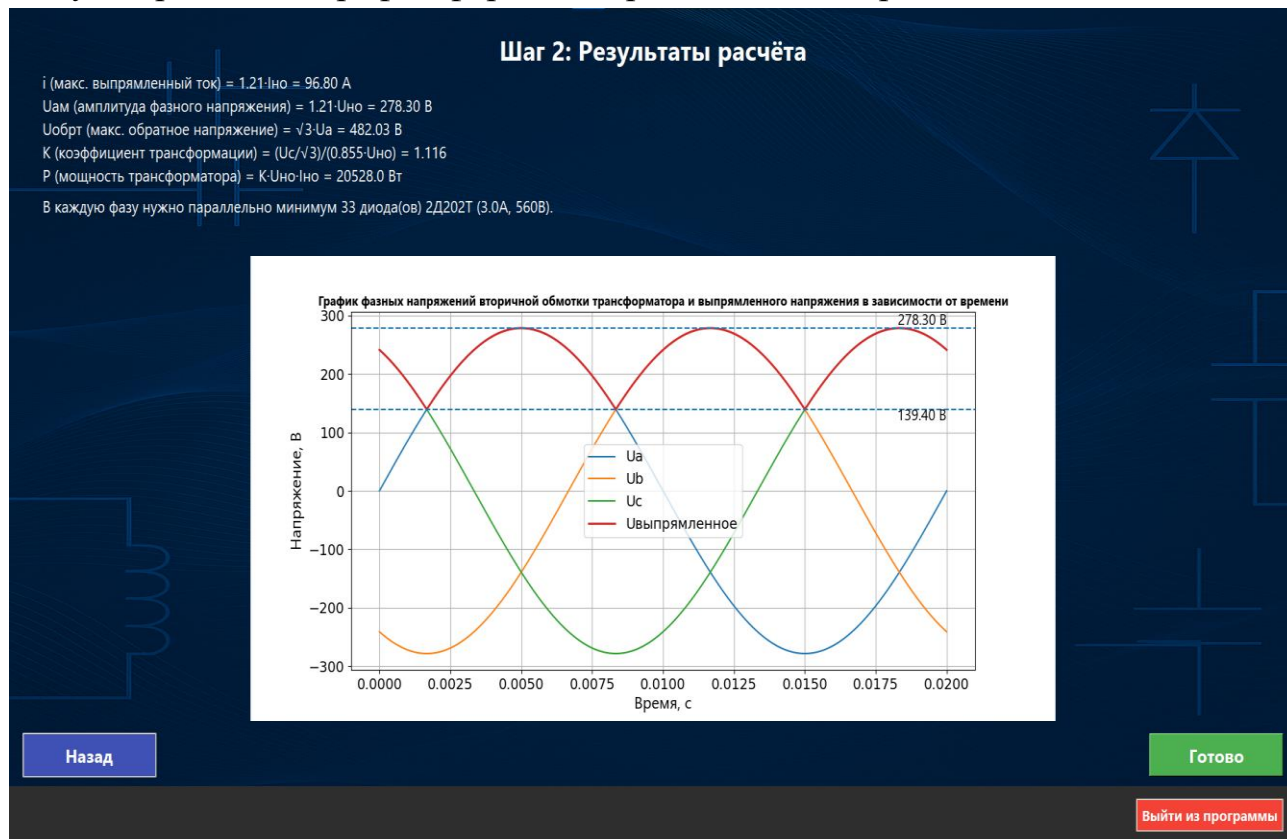


Рис. 3.

Для удобства пользователя реализованы функции возврата к вводу данных и завершения расчётов.

В ходе выполненного исследования была разработана учебная программа для расчёта параметров трёхфазного мостового выпрямителя на диодах. Программа обладает дружелюбным интерфейсом, позволяет автоматически рассчитывать ключевые параметры схемы и визуализировать полученные результаты. Полученные результаты полностью совпадают с расчётами по классическим методикам, что подтверждает корректность работы приложения.

Разработанная программа может использоваться в учебном процессе по дисциплинам «Электротехника» и «Схемотехника». В дальнейшем планируется расширение функциональности за счёт добавления расчётов для других топологий выпрямителей, расширенной визуализации и возможностей сохранения результатов.

Тумашов Евгений Николаевич,

обучающийся 2 курса магистратуры

Инженерно-технологического института ФГБОУ ВО

«Государственный аграрный университет Северного Зауралья».

Научные руководители: И.В. Савчук, к.т.н., доцент, доцент кафедры

энергообеспечения сельского хозяйства; Т.А. Широбокова, к.т.н., доцент

ФГБОУ ВО «Государственный аграрный университет Северного Зауралья»,

г. Тюмень

ПРОЕКТИРОВАНИЕ ЭНЕРГОЭФФЕКТИВНОЙ КАЛОРИФЕРНОЙ СИСТЕМЫ ОТОПЛЕНИЯ ДЛЯ ПРОИЗВОДСТВЕННЫХ ПРЕДПРИЯТИЙ С УЧЕТОМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Цифровизация агропромышленного сектора – одно из направлений развития цифровой экономики, а также стратегическая задача развития страны⁹³.

В современных условиях содержание птицы в промышленных масштабах требует создания стабильного и оптимального микроклимата в помещении. Микроклимат представляет собой совокупность факторов, оказывающих влияние на состояние климата в ограниченном пространстве (в помещении). Поддержание благоприятного микроклимата в помещении с животными обеспечивает сохранность продукции и повышение ее качества⁹⁴. Неправильное поддержание этих параметров влечет за собой ухудшение здоровья птиц и снижение их продуктивности, особенно в зимний период, когда увеличиваются энергозатраты на поддержание оптимальной температуры.

Энергоэффективные системы отопления, такие как калориферы, имеют значительные преимущества для обеспечения стабильного микроклимата. Тем не менее традиционные системы требуют постоянного контроля и не всегда адаптируются к быстро меняющимся условиям. В результате возникает необходимость в проектировании автоматизированной системы, которая могла

⁹³ Указ Президента РФ № 204 от 07.05.2018 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 г.». Программа «Цифровая экономика Российской Федерации» (Распоряжение Правительства РФ от 28.07.2017).

⁹⁴ Довлатов И.М. Автоматизированная система обеспечения микроклимата в птичниках / И.М. Довлатов, Л.Ю. Юферев, В.В. Курсанов, Д.Ю. Павкин, В.Ю. Матвеев // Вестник НГИЭИ. 2018. № 7 (86). С. 7.

бы на основе интеллектуального анализа климатических данных предсказывать изменения и своевременно адаптировать параметры отопления для минимизации энергозатрат.

Целью настоящего исследования является разработка калориферной системы, оснащенной системой интеллектуального управления, которая может адаптировать параметры микроклимата на основе анализа данных о температуре, влажности и погодных условиях. Такой подход предполагает использование сенсоров и методов предиктивной аналитики, что позволяет повысить эффективность системы и снизить себестоимость продукции за счет автоматического регулирования условий содержания птицы.

Однако, активное развитие современных информационных технологий в агропромышленном комплексе Российской Федерации несет и новые риски, требующие современных средств защиты. Данные с умных устройств, передающих и обрабатывающих параметры объектов и их окружения (оборудования и датчиков, измеряющих параметры почвы, растений, микроклимата и др.), БПЛА, спутников и многое необходимо собирать, передавать и обрабатывать. Сейчас большинство проектов используют небезопасные каналы связи и оборудование.

Цифровизация АПК несет в себе следующие угрозы:

1. В случае перехвата команд управления могут быть: подмена данных мониторинга, подмена конфигурационной информации устройств, подмена уставок процесса, эксплуатация уязвимостей IoT-устройств.

2. Экономический ущерб: простои производства, брак продукции, вывод из строя оборудования, затраты на внеплановый ремонт

3. Социальные последствия: некачественная продукция, опасная для жизни людей продукция, атаки на телекоммуникационные инфраструктуры ботнетами из IoT-устройств.

Поэтому, при проектировании умных систем поддержания микроклимата необходимо рассматривать вопросы безопасности информационных систем.

Калориферная система отопления включает теплообменные устройства, которые используют горячую воду или пар для поддержания оптимальной температуры в помещении. Данный подход обеспечивает равномерное распределение тепла и позволяет контролировать условия в зависимости от возраста птицы и погодных условий. Как показано в исследовании А.Х. Сагторова, А.А. Акрамова, А.М. Абдуразакова «Повышение эффективности калорифера, используемого в системе вентиляции», предприятие может сэкономить до 15–20 % потребляемой тепловой энергии существующей водонагревательной системы за счет установки калорифера в системе вентиляции. Кроме того,

достигается повышение теплотворной способности на 15 % без изменения количества потребляемой энергии по сравнению с существующей теплотворной способностью, производимой в простой воде. Кроме того, достигается повышение эффективности работы калорифера на 15 % без изменения количества потребляемой энергии по сравнению с существующим водяным трубчатым калорифером⁹⁵.

В конструкции системы были учтены климатические особенности помещения птицефабрики, включая сезонные колебания температуры и влажности, что особенно важно для зонального контроля. В предложенной системе установлены датчики температуры, влажности и наружного климата, которые обеспечивают непрерывный сбор данных для анализа.

Основу работы системы составляет блок-схема алгоритма интеллектуальной настройки микроклимата, включающая несколько последовательных этапов:

1. Сбор данных с датчиков. Установка датчиков температуры, влажности и других показателей по всей площади помещения позволяет непрерывно собирать информацию, необходимую для корректной работы системы (научная новизна).

2. Предварительная обработка данных. Включает фильтрацию и нормализацию для повышения точности анализа и удаления аномальных значений.

3. Анализ данных и выявление закономерностей. На данном этапе проводится корреляционный анализ и выявляются паттерны изменения параметров, например, суточные колебания температуры.

4. Обучение и применение модели. Модель машинного обучения, построенная на базе исторических данных, прогнозирует изменения температуры и влажности для более точного управления системой.

5. Оптимизация и настройка калориферов. Система адаптирует настройки по зонам, увеличивая или уменьшая мощность обогрева в зависимости от условий в помещении.

6. Обратная связь и корректировка. Обеспечивает контроль в реальном времени и вносит корректировки, если условия отклоняются от заданных параметров.

7. Ручное управление. Предусматривает режим для аварийного вмешательства в случае необходимости.

8. Обновление и дообучение модели. Постоянное накопление данных для улучшения точности прогностической модели.

⁹⁵ Сатторов А.Х., Акрамов А.А., Угли Абдуразаков А.М. Повышение эффективности калорифера, используемого в системе вентиляции // Достижения науки и образования. 2020. № 5. С. 12.



Рис. 1. Блок-схема интеллектуальной настройки микроклимата для калориферной системы отопления.

На основании данных, полученных от интеллектуальной системы анализа, калориферы регулируют температуру и влажность воздуха, предотвращая резкие колебания и обеспечивая стабильный микроклимат. Например, при прогнозировании понижения температуры система увеличивает мощность калориферов в определённых зонах. Если ожидается повышение температуры, мощность нагревателей уменьшается, что позволяет экономить энергию без ущерба для микроклимата.

Кроме того, система позволяет управлять условиями по зонам, выделяя участки для молодняка, которым требуется более тёплый микроклимат, и для взрослой птицы, менее чувствительной к температурным изменениям. Это особенно важно для птицефабрик, где необходимы различные условия для роста птиц на разных этапах. Таким образом, интеллектуальная калориферная система позволяет поддерживать стабильный микроклимат с минимальными затратами, повышая продуктивность и снижая себестоимость производства.

Разработка энергоэффективной калориферной системы отопления на основе интеллектуального анализа климатических данных позволяет создать устойчивый микроклимат в условиях птицефабрики, адаптированный под потребности птицы на разных этапах роста. Применение прогностических моделей машинного обучения для регулирования параметров микроклимата позволяет системе своевременно реагировать на изменения, оптимизируя работу калориферов и снижая затраты на энергоресурсы.

Таким образом, внедрение интеллектуальной калориферной системы отопления позволяет значительно повысить эффективность производства, обеспечивая оптимальные условия для содержания птицы и снижая затраты на энергию на 15–20 %.

Для обеспечения безопасности информационных ресурсов необходимо предусмотреть криптографическую защиту данных, межсетевое экранирование, установку шлюзов безопасности ViPNet. Перечисленные мероприятия будут являться оптимальным средством защиты от несанкционированного доступа к информационным ресурсам и их передаче по каналам связи.

**Хасанов Ильгиз Раушанович,
Лазарева Анастасия Петровна,**

*обучающиеся 3 курса Института нефти и газа
им. М.С. Гуцериева ФГБОУ ВО «УдГУ».*

*Научные руководители: С.А. Хорьков, доцент кафедры теплоэнергетики;
В.В. Зиновьев, старший преподаватель кафедры теплоэнергетики
Удмуртского государственного университета,
г. Ижевск*

СРАВНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ДИАГНОСТИКИ СИЛОВЫХ ТРАНСФОРМАТОРОВ

Силовые трансформаторы преобразуют напряжение при передаче и распределении электроэнергии в энергетической системе. Несмотря на то, что трансформаторы считаются одними из самых надёжных компонентов электрической сети, они подвержены различным видам отказов, связанными как с внутренними, так и с внешними причинами.

Причины отказов трансформаторов могут быть самыми разнообразными – от старения изоляции до производственных дефектов и воздействия внешней среды. Однако особенно опасны те виды повреждений, которые могут привести к аварийным отказам, сопровождающимся пожарами и длительными перебоями в электроснабжении.

Среди наиболее распространённых причин отказов можно выделить:

- отказ диэлектрической изоляции;
- короткие замыкания внутри обмоток;
- перегрев активной части;
- утечки масла и деградация охлаждающей среды;
- воздействие перенапряжений и токов молнии.

К традиционным методам диагностики относят: вибродиагностику, хроматографию растворенных газов в трансформаторном масле, тепловизионный

контроль⁹⁶. Анализ причин отказов показывает, что этих методов недостаточно. Возрастает необходимость точной и своевременной диагностики технического состояния трансформаторов. Использование методов искусственного интеллекта⁹⁷ (ИИ) и машинного обучения (МО) позволяет автоматизировать процесс анализа собранных данных о состоянии трансформатора, выявлять потенциальные неисправности на ранних стадиях и предотвращать аварийные ситуации ещё до их развития. Интеллектуальные системы способны интегрироваться в цифровую инфраструктуру подстанций, обрабатывать данные от многочисленных сенсоров и принимать решения на основе объективных, измеренных показателей.

В частности, для диагностики трансформаторов используют различные алгоритмы машинного обучения⁹⁸. Для оценки расстояний в пространстве диагностируемых параметров применяют различные метрики, такие как евклидово расстояние, расстояние Минковского и манхэттенское расстояние. В практике машинного обучения применяют и другие виды метрик.

В данной работе рассматривается потенциал ИИ в сфере диагностики трансформаторов, ключевые методы анализа технического состояния, а также примеры реализации интеллектуальных систем в энергетике.

Описание данных и параметров измерений

Для анализа технического состояния трансформаторов использовались данные, собранные с помощью устройств Интернета вещей (IoT), установленных на трансформаторных подстанциях. Сбор данных осуществлялся в реальном времени с высокой частотой обновления – каждые 15 минут, в период с 25 июня 2019 года по 14 апреля 2020 года⁹⁹.

Такая высокая частота мониторинга позволяет не только фиксировать текущие значения рабочих параметров, но и проводить их анализ в динамике, выявляя аномалии, тенденции и потенциально опасные отклонения от допустимых значений параметров.

В качестве объекта мониторинга выступает трехфазный трансформатор мощностью 1500 кВА, напряжением 10/0,4 кВ.

⁹⁶ Хренников А.Ю. Высоковольтное оборудование в электротехнических системах: диагностика, дефекты, повреждаемость, мониторинг : учеб. пособие. Москва : ИНФРА-М, 2019.

⁹⁷ Гофман А.В., Ведерников А.С., Дашков В.М. Технологии машинного интеллекта для мониторинга силовых трансформаторов // Энергия единой сети. 2020. № 4 (53). С. 48-55.

⁹⁸ Лютаревич А.Г. Применение нейронных сетей для прогнозирования параметров электропотребления // Вестник Югорского государственного университета. 2023. № 2 (69). С. 124–132.

⁹⁹ Putchala S. Distributed Transformer Monitoring // Kaggle. URL: <https://www.kaggle.com/datasets/sreshta140/ai-transformer-monitoring> (date of application: 10.04.2025).

В перечень отслеживаемых параметров входят следующие параметры: напряжения: фазные VL1, VL2, VL3, линейные VL12, VL23, VL31; токи линейные IL1, IL2, IL3, индикаторы состояния трансформатора: **ОТ** – индикатор температуры масла, **WT** – индикатор температуры обмотки, **АТ** – индикатор температуры окружающей среды, **ОЛ** – индикатор уровня масла, **ОТ_А** – аварийный сигнал индикатора температуры масла, **ОТ_А (trip)** – сигнал отключения по температуре масла, **МОГ_А** – индикатор магнитного датчика уровня масла. Приведенные параметры дают полную картину электрического состояния трансформатора в каждый момент времени.

Конструктивные особенности микропроцессорного устройства сбора данных

Для сбора, обработки и анализа параметров работы трансформатора предложено специализированное микропроцессорное устройство¹⁰⁰. Оно представляет собой компактную систему, включающую в себя датчики, часы реального времени, аналого-цифровой преобразователь, а также плату Z7-Lite 7010, на базе которой реализована программно-аппаратная платформа.

Применяемые датчики:

1. Температурные датчики MLX90614ESF (более трёх):
 - Инфракрасные термометры для бесконтактного измерения температуры объекта.
 - Измеряют как температуру объекта, так и окружающей среды.
2. Комбинированный датчик BME280:
 - Измеряет температуру, давление и влажность воздуха.
3. Энергометр PZEM-004t-100A (шесть штук):
 - Позволяет контролировать переменный ток, напряжение, активную и реактивную мощность, частоту и электропотребление.
4. Аналого-цифровой преобразователь ADS1115:
 - Обеспечивает высокоточное преобразование аналоговых сигналов с датчиков в цифровую форму.

Методы (модели) классификации

Классификация позволяет показать, в каком состоянии находится трансформатор на основе температуры, напряжения, тока и других параметров, которые фиксируют датчики.

В процессе работы была проведена классификация пространства параметров состояния трансформаторов с использованием различных методов (моде-

¹⁰⁰ Громько И.Л., Белькин В.О. Диагностика трансформаторов с помощью приборного учета данных и сверточных нейронных сетей // Исследования и разработки в области машиностроения, энергетики и управления : материалы XXI Международной научно-технической конференции студентов, аспирантов и молодых ученых : в 2-х частях, Гомель, 22–23 апреля 2021 года / под общей редакцией А.А. Бойко. Том Часть 1. Гомель : Гомельский государственный технический университет им. П.О. Сухого, 2021. С. 251-253.

лей) машинного обучения¹⁰¹. Были проанализированы следующие методы (модели) классификации:

- Decision Tree – модель на основе иерархического разбиения признакового пространства;
- Random Forest – ансамблевая модель, основанная на множестве случайно построенных деревьев решений;
- ExtraTreesClassifier – модификация случайного леса с экстремальной случайностью при построении деревьев;
- XGBClassifier – эффективная реализация градиентного бустинга, демонстрирующая высокую точность на табличных данных;
- Logistic Regression – линейный классификатор, основанный на вероятностной модели;
- Support Vector Machines (SVM) – метод построения оптимальной разделяющей гиперплоскости с максимальным зазором.

Формирование моделей было осуществлено на языке программирования общего назначения Python с использованием библиотеки Scikit-learn. Для оценки моделей используется матрица ошибок.

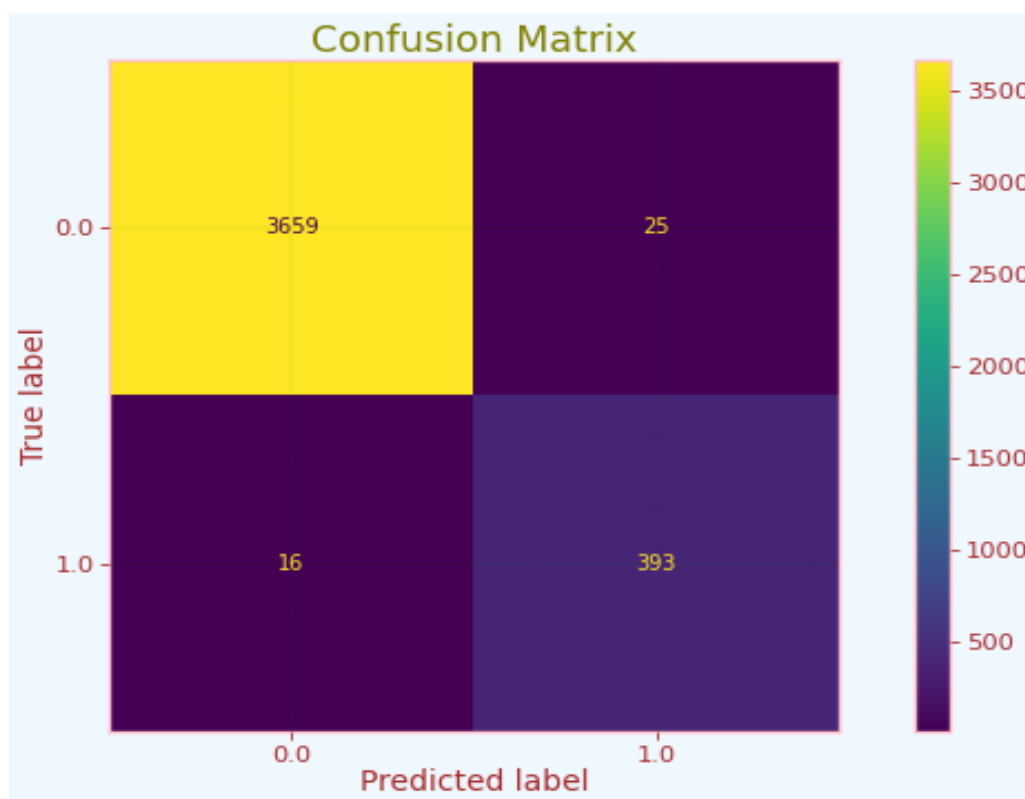


Рис. 1. Матрица ошибок модели Random Forest.

¹⁰¹ Prasojo, Rahman & Akmal, Muhammad & Putra, A & Eka, Meyti & Rahmanto, Anugrah & Ghoneim, Sherif & Mahmoud, Karar & Lehtonen, Matti & Darwish, M. M. F. Precise transformer fault diagnosis via random forest model enhanced by synthetic minority over-sampling technique. 109361. 10.1016/j.ejpsr.2023.109361.

Результаты сравнения моделей классификации.

Model	Training Accuracy	Model Accuracy Score
ExtraTreesClassifier	100.00	99.02
Decision Tree	100.00	99.00
XGBClassifier	100.00	98.80
Random Forest	100.00	98.56
AdaBoostClassifier	98.20	97.83
KNN	95.41	95.55
Logistic Regression	98.08	95.48
Support Vector Machines	94.22	94.28

Она позволяет определить, насколько хорошо модель справляется с поставленной задачей классификации и сравнить её с другими моделями, например, для модели Random Forest матрица приведена на рис. 1.

Матрица ошибок показывает количество правильных и ошибочных предсказаний для каждого класса. Она полезна для анализа ошибок модели. Матрица ошибок позволяет увидеть, долю ошибок типа «ложная тревога» и «пропуск цели». Результаты сравнения моделей сведены в таблицу 1.

Проведён анализ литературных источников и сформирован датасет (структурированный набор данных) на основе открытых данных с платформы Kaggle. Методами машинного обучения реализована классификация параметров состояния трансформаторов. Оценка эффективности моделей осуществлялась на основе матрицы ошибок. Наиболее стабильные и точные результаты продемонстрировала модель ExtraTreesClassifier. Вместе с тем, методы машинного обучения требуют дальнейшего изучения с целью повышения их эффективности при работе с многомерными промышленными данными.

Данное исследование подтверждает высокую эффективность использования искусственного интеллекта и машинного обучения для улучшения диагностики и управления жизненным циклом трансформаторов. Прогнозирование технического состояния и оптимизация режимов работы на основе реальных данных открывают новые возможности для автоматизации процессов управления энергетическими системами, повышения их стабильности и снижения затрат на обслуживание.

Хозеев Илья Ильдарович,

обучающийся 4 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: Т.Н. Стерхова, к.т.н., доцент, доцент кафедры

информационной безопасности в управлении Удмуртского

государственного университета,

г. Ижевск

АВТОМАТИЗАЦИЯ ОБРАБОТКИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Процесс реагирования на инциденты начинается не тогда, когда система уже скомпрометирована, а с этапа подготовки. В связи с этим ключевой необходимостью является автоматическое реагирование и обработка инцидентов информационной безопасности. При обнаружении инцидента первое действие – его изоляция. Зараженные системы должны быть отключены от сети, но не выключены, чтобы сохранить данные в памяти для анализа и минимизации ущерба для объекта в будущем, подверженного атаке или заражению.

Целью научной работы являлось обработка инцидента информационной безопасности, при помощи открытого ПО Suricata¹⁰², реализованного для обеспечения информационной безопасности локальной сети.

Программное обеспечение Suricata было установлено и настроено на виртуальной машине Ubuntu 22.04 в гипервизоре Proxmox.

Suricata имеет следующую структуру правила, для фильтрации трафика в локальной сети: «Действие» – «Протокол» – «Адрес источника» – «Направление» – «Адрес назначения» – «Порт назначения». Пример готового правила:

```
alert tcp any any -> 192.168.1.10 80
```

```
10/25/2023-15:30:45.123456  [**] [1:1000001:1] ICMP Ping to 192.168.1.10 Detected [**] [Classification: Network Scan] [Priority: 3] {ICMP} 192.168.1.5 -> 192.168.1.10
```

Рис. 1. Пример работы правила, результат в журнале fast.log

Данное правило будет регистрировать любой трафик, направленный на хост 192.168.1.10 по порту 80.

¹⁰² Suricata : [Электрон. ресурс]. URL: <https://suricata.io/> (дата обращения: 01.04.2025).

Suricata, являясь универсальным средством IDS/IPS, обладает гибким способом настройки правил, в том числе поддерживает такие форматы, как yaml, json и уага-правила. В том числе, существуют правила в открытых источниках.

Вывод журналов Suricata в формате json, позволяет интегрировать данную систему для работы с Telegram (вывод журналов), интегрировать в инструментарий elasticsearch, интеграция с Даш-борд панелью на основе Kibana.

В следствие того, что Suricata, обладая гибкой настройкой правил, и способностью работать как IPS, т.е. автоматически блокировать попытки вторжения в систему по различным сетевым протоколам, открывается возможность для автоматизации обработки инцидентов информационной безопасности.

Сымитируем Brute-force атаку по протоколу SSH на ресурс. Для этого, создадим правило, которое будет блокировать подключение к виртуальной машине после определенного количества неудачных попыток входа.

```
drop tcp $EXTERNAL_NET any -> $HOME_NET 22 \  
(msg:"IPS: SSH Brute Force Blocked"; \  
flow:to_server,established; \  
content:"SSH-"; nocase; \  
threshold:type both, track by_src, count 5, seconds 60; \  
sid:1000100; rev:1;)
```

```
10/25/2023-14:45:12.345678  [**] [1:1000101:1] IPS: ICMP Flood Blocked [**] [Classification: (no  
ne)] [Priority: 3] {ICMP} 192.168.1.15 -> 10.0.0.5
```

Рис. 2. Правило для автоблокировки трафика по порту 22 и результат в журнале.

Результатом работы такого правила, будет автоматическая блокировка подключения по SSH (22 порт) при пяти и более неудачных входах в систему. Помимо автоматической блокировки, Suricata также оставляет запись в журнале для данного события, что дает возможность для дальнейшего дублирования записи журнала в формате json в другие инструменты, такие как elasticsearch, kibana.

Таким образом, ПО Suricata, обладая гибкой настройкой правил фильтрации трафика и регистрации событий, позволяет автоматизировать процесс обработки инцидента информационной безопасности, посредством средств IPS, встроенных в Suricata.

Шилов Дмитрий Алексеевич,

обучающаяся 4 курса Института права,

социального управления и безопасности ФГБОУ ВО «УдГУ».

Научный руководитель: О.В. Меркушев, к.т.н., доцент кафедры

информационной безопасности в управлении Удмуртского

государственного университета,

г. Ижевск

ЭВОЛЮЦИЯ DevOps (DevSecOps) – ОТ ВИРТУАЛИЗАЦИИ К КОНТЕЙНЕРНОЙ ОРКЕСТРАЦИИ С ПОМОЩЬЮ Docker И Kubernetes

Современные подходы к разработке программного обеспечения требуют интеграции принципов безопасности на всех этапах жизненного цикла. В связи с этим ключевой необходимостью является анализ эволюции DevOps в DevSecOps, включая переход от виртуальных машин к контейнерной оркестрации с использованием Docker и Kubernetes, а также внедрение методологии безопасного построения информационных сетей. Автоматизированное сканирование на уязвимости перед развертыванием контейнеризированных приложений позволяет значительно снизить риски кибератак и обеспечить соответствие современным стандартам информационной безопасности.

Современные ИТ-инфраструктуры активно переходят от традиционных виртуальных машин к контейнерным технологиям, что обусловлено их гибкостью, масштабируемостью и экономичностью. Однако вместе с преимуществами возникают новые вызовы, связанные с безопасностью. DevOps-методологии эволюционируют в направлении DevSecOps, где безопасность становится неотъемлемой частью жизненного цикла разработки и эксплуатации ПО.

Цель исследования – проанализировать эволюцию DevOps-практик, оценить эффективность контейнеризации и оркестрации по сравнению с виртуализацией, а также разработать методику безопасного развертывания приложений с использованием инструментов сканирования уязвимостей.

Для проведения эксперимента была развернута тестовая среда, включающая:

Виртуальные машины (Proxmox) – для сравнения производительности и ресурсопотребления с контейнерами.

Docker-контейнеры – с тестовым веб-приложением (Nginx + Python API).

Кластер Kubernetes (k3s) – для оркестрации контейнеров и автоматического масштабирования.

Инструменты сканирования уязвимостей:

Trivy – для анализа образов Docker.

Clair – для проверки уязвимостей в реестрах контейнеров.

Методика исследования:

Измерение времени развертывания и потребления ресурсов (CPU, RAM) для виртуальных машин и контейнеров.

Нагрузочное тестирование с использованием Locust для оценки производительности Kubernetes.

Сканирование образов Docker на уязвимости и их устранение путем оптимизации Dockerfile.

Результаты эксперимента.

1. Производительность.

Таблица 1

Сравнение виртуализации и контейнеризации.

Параметр	Виртуальные машины	Docker	Kubernetes
Время развертывания	12±2 мин	1.5±0.3 мин	2±0.5 мин
Потребление CPU (ср.)	15 %	5 %	8 % (с учетом оркестрации)
Потребление RAM	2 ГБ	500 МБ	1 ГБ (с учетом Overhead)

2. Безопасность.

Trivy выявил 23 уязвимости (из них 5 критических) в базовом образе Alpine Linux¹⁰³.

После оптимизации Dockerfile (уменьшение слоев, обновление пакетов) количество критических уязвимостей сократилось до 1¹⁰⁴.

Clair подтвердил результаты, обнаружив схожие уязвимости в реестре контейнеров¹⁰⁵.

3. Соответствие стандартам.

Показатели безопасности соответствуют:

ГОСТ Р 57580.1-2017 (безопасность информационных технологий).

NIST SP 800-190 (рекомендации по контейнерной безопасности).

¹⁰³ Trivy Documentation : [Электрон. ресурс] // Aqua Security. URL: <https://trivy.dev/docs/> (дата обращения: 16.05.2025).

¹⁰⁴ ГОСТ Р 57628-2017. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. Введ. 2018-03-01. Москва : Стандартинформ, 2017. IV, 32 с.

¹⁰⁵ Application Container Security Guide: NIST Special Publication 800-190 / National Institute of Standards and Technology. Gaithersburg, 2023. 56 с.

Переход от виртуализации к контейнеризации позволяет значительно сократить время развертывания и потребление ресурсов. Однако контейнерные технологии требуют более строгого контроля безопасности, так как уязвимости в базовых образах могут привести к компрометации всей системы.

Преимущества Kubernetes в DevSecOps:

Автоматическое масштабирование и отказоустойчивость.

Интеграция с инструментами сканирования (Trivy, Clair, Anchore).

Поддержка политик безопасности (PodSecurityPolicy, Network Policies).

Рекомендации:

Использовать минимальные базовые образы (Alpine, Distrosless).

Внедрять SBOM (Software Bill of Materials) для отслеживания зависимостей.

Автоматизировать сканирование уязвимостей в CI/CD (GitLab CI, GitHub Actions).

Проведенное исследование подтвердило эффективность контейнерной оркестрации по сравнению с виртуализацией. Интеграция инструментов безопасности в DevOps-процессы (DevSecOps) позволяет минимизировать риски кибератак и обеспечивает соответствие современным стандартам.

Перспективы дальнейших исследований:

Анализ безопасности serverless-архитектур.

Исследование возможностей eBPF для мониторинга контейнеров.

Разработка автоматизированных политик соответствия GDPR и ISO 27001¹⁰⁶.

¹⁰⁶ Docker Security Best Practices : [Электронный ресурс] // Docker Official Documentation. URL: <https://docs.docker.com/security/> (дата обращения: 16.05.2025).

ОПИСАНИЕ ФУНКЦИОНАЛЬНОСТИ ИЗДАНИЯ

Электронное издание имеет интерактивное содержание, позволяющее переходить к тексту по щелчку компьютерной мыши.

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ:

Минимальные системные требования: Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше; 8x CD-ROM; разрешение экрана 1024×768 или выше; программа для просмотра pdf.

СВЕДЕНИЯ О ЛИЦАХ, ОСУЩЕСТВЛЯВШИХ ТЕХНИЧЕСКУЮ ОБРАБОТКУ И ПОДГОТОВКУ МАТЕРИАЛОВ:

Оформление электронного издания : Издательский центр «Удмуртский университет».

Компьютерная верстка: И.А. Бусоргина

Авторская редакция

Подписано к использованию 10.09.2025
Объем электронного издания 4,4 Мб, тираж 10 экз.
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел. : +7(3412)916-364 E-mail: editorial@udsu.ru
