# Аннотация

Данный документ представляет собой описание исследовательского проекта, направленного на разработку методологии и рекомендаций по написанию безопасного кода с учетом принципов DevSecOps и кибербезопасности. В условиях постоянно меняющегося ландшафта угроз и уязвимостей, важно не только разрабатывать качественное программное обеспечение, но и обеспечивать его защиту на всех этапах жизненного цикла.

Проект включает в себя анализ текущих уязвимостей в процессе разработки программного обеспечения, исследование причин их возникновения и методов предотвращения. Особое внимание уделяется уязвимостям, возникающим на различных этапах жизненного цикла разработки, включая проектирование, кодирование, тестирование, развертывание и эксплуатацию. Также рассматриваются уязвимости, связанные с использованием сторонних библиотек и зависимостей, а также неправильной конфигурацией систем и сервисов.

В документе подробно описаны методы и практики безопасного кодирования, включая минимизацию привилегий, проверку ввода, шифрование данных, использование безопасных библиотек и фреймворков, логирование и мониторинг, а также обработку ошибок и исключений. Применяются рекомендации OWASP для обеспечения безопасности веб-приложений.

Практическая значимость проекта заключается в создании комплексной методологии и набора рекомендаций для написания безопасного кода, которые могут быть использованы разработчиками и специалистами по безопасности для повышения уровня защиты программного обеспечения на всех этапах его жизненного цикла. Результаты проекта могут быть адаптированы для различных предприятий и организаций, занимающихся разработкой программного обеспечения, что позволит им интегрировать практики безопасности в свои процессы разработки и эксплуатации.

Внедрение предложенной методологии и рекомендаций позволит улучшить управление безопасностью кода, упростить внедрение и использование инструментов статического и динамического анализа. Это позволит выявлять и устранять уязвимости на ранних стадиях разработки, что значительно снизит затраты и усилия, связанные с исправлением уязвимостей на поздних этапах.

Таким образом, проект имеет значительный потенциал для коммерческого применения и может быть использован в различных отраслях, где безопасность программного обеспечения является критически важной.