МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2025.155.1

ТЕСТИРОВАНИЕ И АНАЛИЗ УЯЗВИМОСТЕЙ МОБИЛЬНЫХ И ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ «ОБЩИХ КРИТЕРИЕВ»

Научная статья

Милаков А.С.[1, *]
[1] ORCID : 0009-0007-9029-7993;
[1] Студия MissoffDesign, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (as[at]infsecacademy.com)

Аннотация

В статье рассматривается проблематика уязвимости мобильных и веб-приложений, а также угрозы, которые могут нарушить конфиденциальность, целостность и доступность информации. Автор анализирует проблему нарушений безопасности приложений, которая особенно актуальна в финансовой сфере. Решить эту задачу можно путем периодической оценки уязвимостей финансовых приложений. В статье приводится обзор литературы по тематике тестирования и анализа уязвимостей приложений по методике ГОСТ Р ИСО/МЭК 18045-2013. Автор подробно описывает процесс тестирования мобильных и веб-приложений на основе «Общих критериев». В работе рассматривается практика тестирования приложений и сосредоточенный анализ уязвимостей приложений. В статье приводятся практические результаты оценки веб-приложения на уязвимости согласно оценочным уровням доверия (ОУД-4). По результатам тестирования приложений автор приходит к выводу о необходимости внедрения процессов безопасной разработки приложений в компаниях, которые создают программное обеспечение для финансового сектора.

Ключевые слова: мобильные приложения, веб-приложения, банки, финансовые организации, уязвимости, угрозы, модель угроз, оценочный уровень доверия, общие критерии, анализ уязвимостей, статический анализ, динамический анализ, тестирование.

TESTING AND ANALYSIS OF MOBILE AND WEB APPLICATION VULNERABILITIES BASED ON ‘COMMON CRITERIA’

Research article

Milakov A.S.[1, *]
[1] ORCID : 0009-0007-9029-7993;
[1] Studio MissoffDesign, Saint-Petersburg, Russian Federation

* Corresponding author (as[at]infsecacademy.com)

Abstract

The article examines the vulnerability of mobile and web applications, as well as the threats that can violate the confidentiality, integrity and availability of information. The author analyses the problem of application security breaches, which is especially relevant in the financial sphere. This issue can be addressed through periodic vulnerability assessment of financial applications. The paper provides a literature review on the subject of testing and analysing application vulnerabilities according to the methodology of GOST R ISO/IEC 18045-2013. The author describes in detail the process of testing mobile and web applications based on the ‘Common criteria'. The paper discusses the practice of application testing and focused application vulnerability analysis. The workprovides practical results of evaluating a web application for vulnerabilities according to the estimated confidence levels (GTC-4). Based on the results of application testing, the author concludes that it is necessary to implement secure application development processes in companies that create software for the financial sector.

Keywords: mobile applications, web applications, banks, financial organisations, vulnerabilities, threats, threat model, confidence score, common criteria, vulnerability analysis, static analysis, dynamic analysis, testing.

Введение

В условиях бурного развития информационных технологий мобильные и веб-приложения занимают центральное место в жизни современных пользователей, предлагая широкий спектр услуг и функций, начиная от повседневных задач до специализированных финансовых процессов, таких как платежи через системы дистанционного банковского обслуживания (ДБО). Однако, наряду с удобством использования и масштабируемостью, приложения становятся объектом повышенного внимания злоумышленников, что создает серьезные риски для безопасности данных и информационных систем (ИС). В таких условиях возникает необходимость внедрения системных подходов к тестированию и анализу уязвимостей программного обеспечения с целью повышения уровня защищенности ИС.

Одним из наиболее признанных международных стандартов в области оценки безопасности программного обеспечения являются «Общие критерии» (Common Criteria for Information Technology Security Evaluation, CC), которые позволяют унифицировать процессы тестирования и сертификации программного обеспечения [2]. В Российской Федерации эта методология издана в виде национальных стандартов [6], [7], [8]. Данные стандарты представляют собой универсальный инструмент для оценки уровня безопасности программного обеспечения,

учитывающий широкий спектр угроз и уязвимостей, а также их потенциальное воздействие на информационные системы.

«Общие критерии» обеспечивают независимую оценку безопасности продуктов и помогают определить соответствие заявленным требованиям безопасности.

Настоящая статья посвящена исследованию и анализу уязвимостей мобильных и веб-приложений с использованием методологии «Общих критериев». Выбор методологии для исследований был сделан автором в предыдущей работе [1], там же даны обоснования этому выбору и расписана теория и практика оценки приложений по оценочному уровню доверия (ОУД-4). В работе рассматриваются ключевые аспекты проведения тестирования, включая анализ методологии, изучение угроз и векторов атак, а также оценка их влияния на безопасность конечных пользователей.

Данная работа является логическим продолжением работы [1] и посвящена практическим аспектам тестирования приложений по ГОСТ Р ИСО/МЭК 18045-2013 [4], таким как функциональное тестирование ATE_FUN, выборочное независимое тестирование ATE_IND и сосредоточенный анализ уязвимостей AVA_VAN.

Метод научных исследований

Автор применяет в этой работе публикационный метод прогнозирования и экспертных оценок, а также использует свой большой опыт в сканировании уязвимостей мобильных и веб-приложений. Научное исследование проводилось следующим образом:

1. Обзор литературных источников по тематике безопасности приложений.
2. Обоснование выбора методологии исследования безопасности приложений на базе «Общих критериев».
3. Краткий обзор методики анализа безопасности приложений на основе «Общих критериев» (ATE_FUN, ATE_IND, AVA_VAN).
4. Инструментальный SAST-анализ (Static application security testing, SAST) веб-приложения.

Цели научной статьи:

1) проанализировать литературу по оценке безопасности мобильных и веб-приложений, рассмотреть нормативные документы в этой области;

2) кратко описать методологию оценки мобильных и веб-приложений, а именно ATE_FUN, ATE_IND и AVA_VAN;

3) провести инструментальный SAST-анализ веб-приложения и оценить его результаты.

Основные ограничения научного исследования: необходимо принять во внимание, что реальные коммерческие работы по тестированию ДБО и других финансовых приложений имеют конфиденциальный характер и подпадают под действие «Соглашений о неразглашении» (NDA), поэтому инструментальный SAST-анализ будет проводиться на тестовом веб-приложении.

Обзор литературных источников по тестированию приложений

В работе [1] детально описана методология оценки мобильных и веб-приложений в финансовом секторе на базе «Общих критериев». В статье кратко описываются другие системы оценки, к примеру, OWASP, NIST, ISO/IEC 27001, однако автор, опираясь на нормативную документацию [2], [4], [6], [9], приходит к выводу о необходимости использования оценки мобильных и веб-приложений финансового сектора по ОУД-4.

В исследовании [3] авторы проводят подробное сравнение методологий OWASP и ГОСТ Р ИСО/МЭК 18045-2013, выделяя преимущества и недостатки каждой методологии. Авторы [3] советуют применять OWASP, но при анализе мобильных и веб-приложений банковского сектора в РФ исследователь в первую очередь должен руководствоваться нормативными документами регулятора, т.е. Банка России. Это значит, что для оценки финансовых приложений стоит выбрать ГОСТ Р ИСО/МЭК 18045-2013 [4].

В работе [5] однозначно рекомендуется методология на базе «Общих критериев», которая очень хорошо подходит для проведения сертификационных испытаний приложений.

С точки зрения анализа и исследования самой методологии «Общих критериев» интересны выводы, сделанные в исследовании M. Kara [10]. Стандарты на основе «Общих критериев» предлагают унифицированный процесс оценки функций безопасности, который помогает систематически выявлять уязвимости в приложениях. «Общие критерии» объединяют различные аспекты безопасности, включая моделирование угроз и управление рисками, обеспечивая целостное представление о защите приложений от угроз.

«Использование вероятностного подхода к оценке рисков помогает разработчикам лучше понять потенциальное влияние уязвимостей приложений», — такие выводы делаются в работе [11].

Открытый стандарт для оценки степени опасности уязвимостей (Common Vulnerability Scoring System, CVSS) помогает приоритизировать уязвимости в зависимости от их потенциального воздействия и эффективно направлять усилия по их исправлению [12].

Практические статьи [14], [15], [16] показывают сам процесс оценки приложений финансового сектора на базе семейства стандартов [6], [7], [8] и [4] с точки зрения разработчика программного обеспечения и оценщика (в терминологии [4]). В работе [16] делается вывод о необходимости проведения выборочного независимого тестирования ATE_IND в финансовой организации.

Статья [17] интересна тем, что напоминает о необходимости проверки на безопасность не только самого приложения, но и его интерфейсов с другими ИС. Эти данные исследователь, как правило, обосновывает в «Функциональной спецификации» проекта.

Анализируя источники, автор приходит к выводу о наличии двух подходов для обеспечения безопасности приложений:

1. Периодический аудит приложений по выбранной методике и на базе нормативных документов регулятора.
2. Организация процесса безопасной разработки ПО «Secure Software Development Life Cycle» (Secure SDLC).

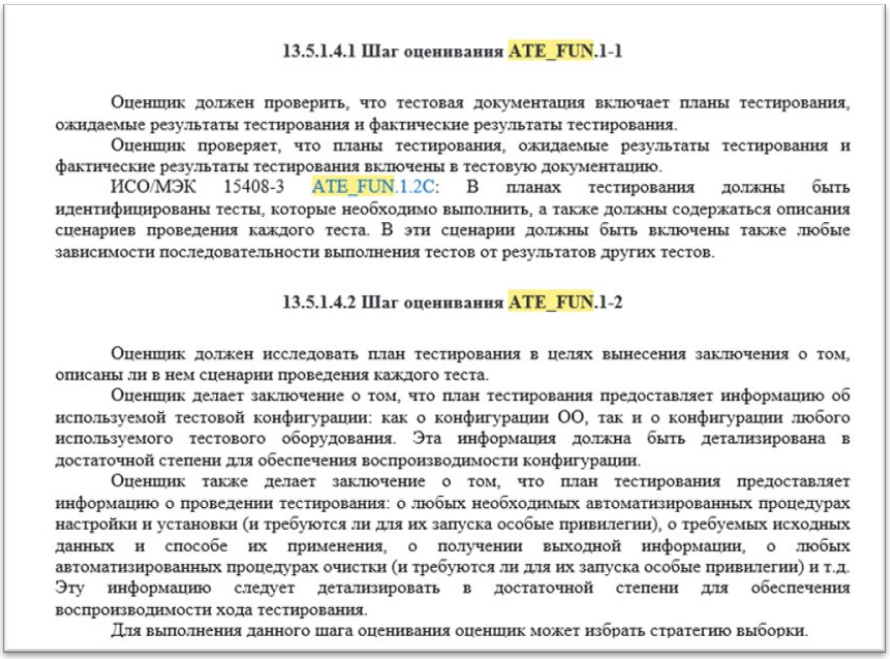
Второй путь подробно рассматривается в методическом пособии [13].

Функциональное тестирование ATE_FUN

Функциональное тестирование ATE_FUN представляет собой процесс оценки того, соответствует ли программное обеспечение заявленным функциональным требованиям безопасности (ФТБ) и ожиданиям, описанным в его «Функциональной спецификации». В рамках этой процедуры проверяется, работают ли все заявленные функции безопасности объекта оценки (ФБО) корректно и предсказуемо в соответствии с их назначением. Функциональное тестирование ATE_FUN является одной из ключевых стадий сертификации программного обеспечения по международному стандарту Common Criteria (ISO/IEC 15408) [2].

С точки зрения Разработчика, на этом этапе необходимо предоставить тест-кейсы, которые должны быть повторяемы, а результаты их воспроизводимы.

В нормативной документации [4] подробно расписаны все шаги Оценщика по контролю тестирования Разработчика. Ниже на рис. 1 дан пример из ГОСТ подобных шагов оценки.



13.5.1.4.1 Шаг оценивания ATE_FUN.1-1

Оценщик должен проверить, что тестовая документация включает планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

Оценщик проверяет, что планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования включены в тестовую документацию.

ИСО/МЭК 15408-3 ATE_FUN.1.2C: В планах тестирования должны быть идентифицированы тесты, которые необходимо выполнить, а также должны содержаться описания сценариев проведения каждого теста. В эти сценарии должны быть включены также любые зависимости последовательности выполнения тестов от результатов других тестов.

13.5.1.4.2 Шаг оценивания ATE_FUN.1-2

Оценщик должен исследовать план тестирования в целях вынесения заключения о том, описаны ли в нем сценарии проведения каждого теста.

Оценщик делает заключение о том, что план тестирования предоставляет информацию об используемой тестовой конфигурации: как о конфигурации ОО, так и о конфигурации любого используемого тестового оборудования. Эта информация должна быть детализирована в достаточной степени для обеспечения воспроизводимости конфигурации.

Оценщик также делает заключение о том, что план тестирования предоставляет информацию о проведении тестирования: о любых необходимых автоматизированных процедурах настройки и установки (и требуются ли для их запуска особые привилегии), о требуемых исходных данных и способе их применения, о получении выходной информации, о любых автоматизированных процедурах очистки (и требуются ли для их запуска особые привилегии) и т.д. Эту информацию следует детализировать в достаточной степени для обеспечения воспроизводимости хода тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Рисунок 1 - Шаги оценивания ATE_FUN

DOI: https://doi.org/10.60797/IRJ.2025.155.1.1

Примечание: ГОСТ Р ИСО/МЭК 18045-2013

Далее, для определения сути процедуры ATE_FUN необходимо воспользоваться уже написанным для проекта «Заданием по безопасности», а именно, функциональными требованиями безопасности (ФТБ) и требованиями доверия к безопасности [1].

На первом этапе тестирования специалисты по безопасности приложений анализируют всю документацию программного продукта, включая «Задание по безопасности», «Функциональную спецификацию», «Базовый модульный проект» и т.д [1]. Это необходимо для того, чтобы понять, какие функции системы должны быть протестированы. ГОСТ Р ИСО/МЭК 18045-2013 указывает, что документация должна быть достаточно подробной, чтобы оценить полноту и корректность выполнения функций. Особое внимание обращается на ФТБ, именно они проверяются в первую очередь на тестировании.

На основе анализа документации формируются тест-кейсы, которые определяют конкретные сценарии использования программного обеспечения. Тест-кейсы разрабатываются таким образом, чтобы охватить как нормальные условия эксплуатации, так и пограничные случаи, в которых система должна корректно работать. Этот шаг критически важен, так как он определяет, насколько полно и тщательно будут протестированы все аспекты функциональности ПО.

На следующем этапе происходит запуск приложения в реальных условиях или с использованием тестовых окружений, приближенных к рабочим (в тестовой среде). Выполняются все разработанные тест-кейсы, и фиксируются результаты каждого теста — успешное выполнение функции или ошибка. Важно отметить, что стандарт [4] подчеркивает необходимость выполнения тестов как в обычных условиях эксплуатации, так и в условиях, близких к реальным угрозам или атакам, чтобы удостовериться, что ПО будет устойчиво и безопасно.

После выполнения тестов результаты сопоставляются с ожидаемыми выводами, которые были определены в «Задании по безопасности» на этапе выработки функциональных требований безопасности. При обнаружении отклонений выполняется дополнительный анализ с целью определения источника ошибок и корректировок.

Финальная часть процедуры заключается в составлении отчета о проведенном функциональном тестировании. В нем должны быть отражены все пройденные тест-кейсы, результаты выполнения каждого из них, а также рекомендации по доработке системы в случае обнаружения несоответствий.

Выборочное независимое тестирование ATE_IND

Выборочное независимое тестирование (ATE_IND) согласно [4] представляет собой методику проверки приложений, при которой сторонняя независимая организация или группа инженеров по безопасности приложений (Оценщик) проверяет некоторые (выборочные) аспекты ИС на соответствие функциональным требованиям безопасности, заявленным в документации на ПО. Это тестирование является неотъемлемой частью оценки безопасности продукта в рамках стандарта Common Criteria [2], и его главная цель — подтвердить корректность работы заявленных ФБО и убедиться в отсутствии уязвимостей или ошибок, которые могут не быть очевидны при внутреннем тестировании (выполненным Разработчиком).

На оценку Разработчик должен предоставить следующую документацию: «Задание по безопасности», «Функциональную спецификацию», «Руководство пользователя», «Руководство по установке ПО» (если есть) и непосредственно сам объект оценки (ОО). Ниже на рис. 2 приведен пример из ГОСТ подобных шагов оценки по ATE_IND.

13.6.1.4.3 Шаг оценивания ATE_IND.1-5

Оценщик должен провести тестирование.

Оценщик использует разработанную тестовую документацию как основу для выполнения тестов по отношению к ОО. Тестовая документация используется как основа для тестирования, но это не мешает оценщику выполнить дополнительные специальные тесты. Оценщик может разработать новые тесты, исходя из режима функционирования ОО, обнаруженного в процессе тестирования. Эти новые тесты заносятся в тестовую документацию.

13.6.1.4.4 Шаг оценивания ATE_IND.1-6

Оценщик должен зафиксировать следующую информацию о тестах, которые составляют подмножество тестирования:

a) идентификационную информацию тестируемого режима выполнения интерфейса;

b) инструкции по подключению и настройке всего требуемого тестового оборудования для проведения конкретного теста;

c) инструкции по установке всех предварительных условий выполнения теста;

d) инструкции по инициированию функции безопасности;

e) инструкции по наблюдению режима выполнения интерфейса;

f) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;

g) инструкции по завершению тестирования и установке необходимого послетестового состояния ОО;

h) фактические результаты тестирования.

Необходимо, чтобы уровень детализации был таким, чтобы другой оценщик мог повторить тесты и получить эквивалентный результат. Хотя некоторые специфические детали результатов выполнения теста могут отличаться (например поля времени и даты в записи аудита), рекомендуется, чтобы общие результаты были идентичными.

Возможны случаи, когда нет необходимости предоставлять всю информацию, представленную на этом шаге оценивания (например фактические результаты тестирования могут не требовать какого бы то ни было анализа до их сравнения с ожидаемыми результатами). Решение опустить эту информацию, как и его логическое обоснование, остается за оценщиком.

Рисунок 2 - Шаги оценивания ATE_IND

DOI: https://doi.org/10.60797/IRJ.2025.155.1.2

Примечание: ГОСТ Р ИСО/МЭК 18045-2013

Выборочное независимое тестирование проводится сторонней группой, не участвовавшей в разработке или тестировании продукта, в терминологии ГОСТ [4] такая группа специалистов именуется — «Оценщик». Подобная группа обладает «свежим взглядом», глубокими компетенциями в сфере информационной безопасности и не связана с предвзятыми представлениями о работе системы, которые могут быть у разработчиков или внутренней команды тестировщиков. Независимые тестировщики должны иметь доступ к документации и спецификациям системы, а также к результатам предыдущих этапов тестирования.

Оценщик анализирует существующие тестовые сценарии (тест-кейсы), которые были разработаны для функционального тестирования (ATE_FUN). Основная задача — определить, какие из них необходимо повторить, а какие части системы требуют создания новых тестов, возможно, для проверки пограничных случаев или других критически важных аспектов.

Инженеры выполняют тестирование на основе подготовленных и уже существующих тест-кейсов. Особенностью независимого тестирования является его направленность на выборочные участки системы. Это означает, что не все функции проверяются, а только те, которые независимые тестировщики сочли важными или подозрительными с точки зрения потенциальных уязвимостей. Также проводится проверка сценариев использования системы в условиях

нестандартных и экстремальных нагрузок, что помогает выявить уязвимости, не всегда очевидные при обычной эксплуатации.

Результаты выборочных тестов сравниваются с результатами тестов Разработчика, а также с документацией (ЗБ и др.) и заявленными функциональными требованиями безопасности. Если независимые тестировщики находят расхождения, ошибки или уязвимости, то они тщательно их документируют. Это важная часть процесса, поскольку независимое тестирование может выявить проблемы, которые не были обнаружены на предыдущих этапах проверки ИС на безопасность.

По завершении выборочного независимого тестирования составляется отчет, содержащий полное описание всех выполненных тестов, их результатов и рекомендаций по устранению выявленных проблем.

Необходимо отметить, что при выполнении оценки на ОУД-4 выборочное независимое тестирование ATE_IND проводится не всегда, однако нормативные документы [4], [8] требуют проведение независимого аудита финансовых приложений. Преимущества независимой экспертизы:объективность оценки, выявление скрытых уязвимостей (не выявленных Разработчиком), повышение доверия к безопасности продукта.

Сосредоточенный анализ уязвимостей AVA_VAN

Сосредоточенный анализ уязвимостей (AVA_VAN) согласно ГОСТ Р ИСО/МЭК 18045-2013 представляет собой комплексную процедуру анализа программного обеспечения с целью выявления потенциальных уязвимостей, которые могут быть использованы злоумышленниками для компрометации системы. Этот анализ является важным элементом сертификации программного обеспечения по стандартам Common Criteria (ISO/IEC 15408), и его главная цель — обнаружить и оценить слабые места системы, которые могут представлять угрозу для её безопасности.

Первым шагом в процедуре AVA_VAN является создание модели угроз, исходя из того, как система будет использоваться, какие компоненты могут быть атакованы, и какие потенциальные векторы атак возможны. Модель угроз создается аналитиком на этапе написания «Задания по безопасности». Для финансовых приложений она, как правило, составляется на основе нормативного документа Банка России [9].

Специалисты по безопасности должны определить возможные сценарии атак, основанные на предполагаемых возможностях и мотивации злоумышленника. ГОСТ [4] требует проведения тщательного анализа сценариев атак, который учитывает реальные риски для конкретного программного обеспечения и среды его функционирования.

На основе модели угроз проводится анализ архитектуры системы и исходного кода, чтобы выявить потенциальные уязвимости. На этом этапе специалисты проверяют, насколько безопасно реализованы ключевые функции системы, как обрабатываются данные пользователей, насколько безопасно организована работа с внешними интерфейсами, и как эффективно реализованы механизмы защиты. Анализ архитектуры позволяет выявить потенциальные уязвимости, связанные с логикой работы системы, её структурой и взаимодействием между компонентами. Все эти моменты аналитик излагает в документе «Описание архитектуры безопасности», а инженер по ИБ проверяет описанное на практике.

Также составляется модель нарушителя, как правило, при проведении ОУД-4 — это «нарушитель с усиленным базовым потенциалом». Ниже в табл. 1 приведена таблица для составления подобной модели.

Таблица 1 - Рейтинг уязвимостей и уровень стойкости ОО

DOI: https://doi.org/10.60797/IRJ.2025.155.1.3

Диапазон значений	Потенциал нападения, требуемый для использования сценария	ОО противостоит нарушителю с потенциалом нападения	Удовлетворяет требованиям компонентов доверия	Не удовлетворяет требованиям компонентов
0-9	Базовый	Не противостоит	-	AVA_VAN. 1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA VAN.5
10-13	Усиленный базовый	Базовый	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA VAN.5
14-19	Умеренный	Усиленный базовый	AVA_VAN.1, AVA_VAN.2, AVA VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	Высокий	Умеренный	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA VAN.4	AVA_VAN.5
=>25	За пределами	Высокий	AVA_VAN.1,	-

Диапазон значений	Потенциал нападения, требуемый для использования сценария	ОО противостоит нарушителю с потенциалом нападения	Удовлетворяет требованиям компонентов доверия	Не удовлетворяет требованиям компонентов
	высокого		AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA VAN.5	

Примечание: ГОСТ Р ИСО/МЭК 18045-2013

На следующем этапе тестировщики имитируют атаки на систему, используя специальное ПО (сканеры уязвимостей). Важно, что AVA_VAN фокусируется не только на типичных уязвимостях (например, ошибки ввода-вывода или неправильное управление памятью), но также и на более сложных, связанных с комбинацией различных уязвимостей и особенностей системы. Такие тесты могут включать:

- Физические атаки (проверка устойчивости системы к манипуляциям с аппаратной частью).
- Социальную инженерию (попытки обмана пользователей системы для получения доступа).
- Атаки на сетевые интерфейсы (проверку на наличие уязвимостей в сетевых протоколах или механизмах аутентификации).

После обнаружения уязвимостей проводится их оценка с точки зрения потенциального ущерба и вероятности успешной эксплуатации. ГОСТ [4] требует классификации уязвимостей по их степени опасности. Уязвимости могут быть разделены на следующие категории:

- Высокий риск: уязвимости, которые могут быть легко использованы злоумышленниками и нанести серьёзный ущерб системе или данным.
- Средний риск: уязвимости, которые требуют значительных усилий для эксплуатации, но могут привести к серьёзным последствиям.
- Низкий риск: уязвимости, которые либо трудны для эксплуатации, либо имеют незначительные последствия.

Кроме этого, исследователь сразу же выделяет критические уязвимости, которые требуют немедленного устранения разработчиками системы. Такая классификация позволяет разработчикам сосредоточить усилия на исправлении наиболее критичных проблем.

Завершающий этап анализа — это предоставление рекомендаций по устранению выявленных уязвимостей. Эксперты предлагают конкретные меры по улучшению безопасности системы, которые могут включать:

- Усиление контроля доступа и улучшение методов аутентификации.
- Защиту данных от несанкционированного доступа (например, шифрование данных).
- Исправление ошибок в коде и архитектуре.
- Введение дополнительных механизмов мониторинга и оповещения о подозрительной активности.

AVA_VAN позволяет глубоко анализировать систему на предмет уязвимостей, что существенно повышает её защищённость перед реальными атаками. Модель угроз и модель нарушителя, используемые в анализе, позволяют сосредоточиться на наиболее значимых для конкретной системы атаках, что делает тестирование более релевантным и эффективным. Проведение AVA_VAN является необходимым для проверки приложения по стандартам Common Criteria [2], что повышает доверие к продукту на международном уровне.

Тестирование веб-приложения и документирование результатов проверки

7.1. Проведение тестирования AVA_VAN

Для проверки предоставляется объект оценки, в который включены внешние домены и IP-адреса, веб-интерфейс сайта test.missoff.ru.

Исследуемый объект (ОО) — это веб-приложение, состоящее из следующих основных компонентов и технологий:

· Основной фронтэнд веб-приложения — содержит код для отображения и обработки клиентской части, включая основной функционал и взаимодействие с пользователем на сайте.

· Веб-сайт — информационная часть веб-приложения, разработанная для отображения статических страниц и предоставления базовой информации пользователям.

Программные компоненты веб-приложения реализованы с использованием следующих технологий:

• JavaScript, TypeScript — используются для динамической обработки данных на стороне клиента и взаимодействия в webview.

• PHP — применяется для реализации серверной логики и обработки запросов пользователя.

Ниже опишем применяемый инструментарий инженера по безопасности приложений.

Статическое сканирование SAST направлено на анализ исходного кода приложения (без его выполнения). При осуществлении SAST инженер по ИБ использует статические анализаторы Sonarsource SonarQube CE и Semgrep для веб-приложений. Sonarsource SonarQube CE — сканер исходного кода, осуществляющий проверку компонентов для выявления уязвимостей и нарушений качества кода. Semgrep — инструмент статического анализа кода с открытым исходным кодом, поддерживающий гибкие правила для обнаружения уязвимостей в различных языках программирования.

Дополнительно также использовались следующие инструменты для тестирования: Nikto, Nmap, SQLmap, OWASP ZAP (Zed Attack Proxy), Nessus, Burp Suite, testssl.sh. Все эти инструменты позволяют выполнить комплексный анализ безопасности веб-приложения и сетевой инфраструктуры, обеспечив выявление и документирование потенциальных уязвимостей.

Далее специалист по ИБ применяет метод триажа (фр. triage — сортировка), а именно, занимается сортировкой уязвимостей. Как было описано выше — это критические уязвимости, а также уязвимости с высоким риском эксплуатации, средним и низким. Также на этапе триажа отделяются положительные срабатывания сканера от ложных срабатываний.

Затем специалист переходит к ручному анализу уязвимостей по методикам OWASP (Open Worldwide Application Security Project). Оценка критичности уязвимостей проводится по CVSS 4.0 (Common Vulnerability Scoring System), по OWASP и по Банку данных угроз (БДУ ФСТЭК РФ).

Ниже приведены примеры найденных уязвимостей веб-приложения test.missoff.ru. Был проведен фокусированный анализ каждого вхождения с риск-фактором СРЕДНИЙ или выше, краткая выборка результатов отчета приведена в Таблице 2.

Таблица 2 - Основной фронтэнд веб-приложения

DOI: https://doi.org/10.60797/IRJ.2025.155.1.4

Risk=Высокий, Confidence=Средний (1) *test.missoff.ru* *SQL-инъекция* *POST test.missoff.ru/auth/?forgot_password=yes*		
1	Alert tags	OWASP_2021_A03 WSTG-v42-INPV-05 OWASP_2017_A01
-	Alert description	Возможна SQL-инъекция. Результаты страницы были успешно обработаны с помощью логических условий [foo-bar@example.com AND 1=1 --] и [foo-bar@example.com AND 1=2 --]
-	Other info	Изменяемое значение параметра было удалено из вывода HTML для целей сравнения. Данные были возвращены для исходного параметра. Уязвимость была обнаружена путем успешного ограничения исходно возвращаемых данных путем изменения параметра
-	Request	*Request line and header section (409 bytes)* *POST https://test.missoff.ru/auth/?forgot_password=yes HTTP/1.1* *Host: test.missoff.ru* *User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0* *Pragma: no-cache* *Cache-Control: no-cache* *Content-Type: application/x-www-form-urlencoded* *Referer: https://test.missoff.ru/auth/?forgot_password=yes* *Content-Length: 164*

Risk=Высокий, Confidence=Средний (1) *test.missoff.ru* *SQL-инъекция* *POST test.missoff.ru/auth/?forgot_password=yes*		
		Cookie: PHPSESSID=F7R4bx1rPyFYyafEHwKQ53NQgFyfFFZc *Request body (164 bytes)* *backurl=%2Fauth%2F&AUTH_FORM=Y&TYPE=SEND_PWD&USER_LOGIN=foo-bar%40example.com+AND+1%3D1+--+&USER_EMAIL=&send_account_info=%D0%92%D1%8B%D1%81%D0%BB%D0%B0%D1%82%D1%8C*
-	Response	Status line and header section (576 bytes) *HTTP/1.1 200 OK* *Server: nginx/1.26.1* *Date: Mon, 04 Nov 2024 20:47:33 GMT* *Content-Type: text/html; charset=UTF-8* *Connection: keep-alive* *X-Powered-By: PHP/7.4.33* *P3P: policyref="/bitrix/p3p.xml", CP="NON DSP COR CUR ADM DEV PSA PSD OUR UNR BUS UNI COM NAV INT DEM STA"* *X-Powered-CMS: Bitrix Site Manager (39d0fb00176e19ac87e87d99529f6e3f)* *Expires: Thu, 19 Nov 1981 08:52:00 GMT* *Cache-Control: no-store, no-cache, must-revalidate* *Pragma: no-cache* *Set-Cookie: PHPSESSID=F7R4bx1rPyFYyafEHwKQ53NQgFyfFFZc; path=/; HttpOnly* *Vary: Accept-Encoding* *Content-Length: 8600* Response body (8600 bytes)

Risk=Высокий, Confidence=Средний (1) *test.missoff.ru* *SQL-инъекция* *POST test.missoff.ru/auth/?forgot_password=yes*		
-	Parameter	*USER_LOGIN*
-	Attack	*foo-bar@example.com AND 1=1 --*
-	Solution	· Не доверяйте вводу на стороне клиента, даже если есть проверка на стороне клиента. · В основном, тип проверки всех данных на стороне сервера. · Если приложение использует JDBC, используйте PreparedStatement или CallableStatement · с параметрами, передаваемыми через '?' · Если приложение использует ASP, используйте объекты команд ADO (ADO Command Objects) со строгой проверкой типов и параметризованными запросами. Если можно использовать хранимые процедуры базы данных (Stored Procedures), используйте их. · Не объединяйте строки в запросы в хранимой процедуре и не используйте 'exec', 'exec немедленно' или аналогичные функции! · Не создавайте динамические запросы SQL, используя простую конкатенацию строк. · Экранировать все данные, полученные от клиента. · Примените «разрешенный список» разрешенных символов или «запрещающий список» запрещенных символов при вводе пользователем. · Применяйте принцип наименьших привилегий,

Risk=Высокий, Confidence=Средний (1) *test.missoff.ru* *SQL-инъекция* *POST test.missoff.ru/auth/?forgot_password=yes*		
		используя наименее привилегированного пользователя базы данных. · В частности, избегайте использования пользователей базы данных «sa» или «db-owner». Это не устраняет SQL-инъекцию, но сводит к минимуму ее влияние. Предоставьте приложению минимальный доступ к базе данных
· *Risk=Средний, Confidence=Высокий* *test.missoff.ru* *Заголовок Content Security Policy (CSP) не задан* *GET test.missoff.ru/robots.txt*		
2	Alert tags	OWASP_2021_A05 OWASP_2017_A06
-	Alert description	Политика безопасности содержимого (CSP) — это дополнительный уровень безопасности, который помогает обнаруживать и смягчать определенные типы атак, включая межсайтовые сценарии (XSS) и атаки с внедрением данных. Эти атаки используются для всего: от кражи данных до порчи сайта или распространения вредоносных программ. CSP предоставляет набор стандартных HTTP-заголовков, которые позволяют владельцам веб-сайтов объявлять утвержденные источники контента, которые браузеры должны разрешить загружать на эту страницу. Охватываемые типы включают JavaScript, CSS, HTML-фреймы, шрифты, изображения и встраиваемые объекты, такие как апплеты Java. ActiveX, аудио и видео файлы.

Risk=Высокий, Confidence=Средний (1) *test.missoff.ru* *SQL-инъекция* *POST test.missoff.ru/auth/?forgot_password=yes*		
-	Other info	—
-	Request	*Request line and header section (211 bytes)* *GET https://test.missoff.ru/robots.txt HTTP/1.1* *Host: test.missoff.ru* *User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0* *Pragma: no-cache* *Cache-Control: no-cache* *Request body (0 bytes)*
-	Response	*Status line and header section (560 bytes)* *HTTP/1.1 404 Not Found* *Server: nginx/1.26.1* *Date: Mon, 04 Nov 2024 20:35:39 GMT* *Content-Type: text/html; charset=UTF-8* *Connection: keep-alive* *X-Powered-By: PHP/7.4.33* *P3P: policyref="/bitrix/p3p.xml", CP="NON DSP COR CUR ADM DEV PSA PSD OUR UNR BUS UNI COM NAV INT DEM STA"* *X-Powered-CMS: Bitrix Site Manager (39d0fb00176e19ac87e87d99529f6e3f)* *Expires: Thu, 19 Nov 1981 08:52:00 GMT* *Cache-Control: no-store, no-cache, must-revalidate* *Pragma: no-cache* *Set-Cookie: PHPSESSID=F7R4bx1rPyFYyafEHwKQ53NQgFyfFFZc; path=/; HttpOnly* *Content-Length: 5238* *Response body (5238 bytes)*

Risk=Высокий, Confidence=Средний (1) *test.missoff.ru* *SQL-инъекция* *POST test.missoff.ru/auth/?forgot_password=yes*		
-	Parameter	—
-	Attack	—
-	Solution	Убедитесь, что ваш веб-сервер, сервер приложений, балансировщик нагрузки и т. д. настроены для установки заголовка Content-Security-Policy для достижения оптимальной поддержки браузера: «Content-Security-Policy» для Chrome 25+, Firefox 23+ и Safari 7. +, «X-Content-Security-Policy» для Firefox 4.0+ и Internet Explorer 10+ и «X-WebKit-CSP» для Chrome 14+ и Safari 6+.

Далее на рисунках 3-5 приведены уязвимости, которые были найдены при исследовании веб-сайта test.missoff.ru.

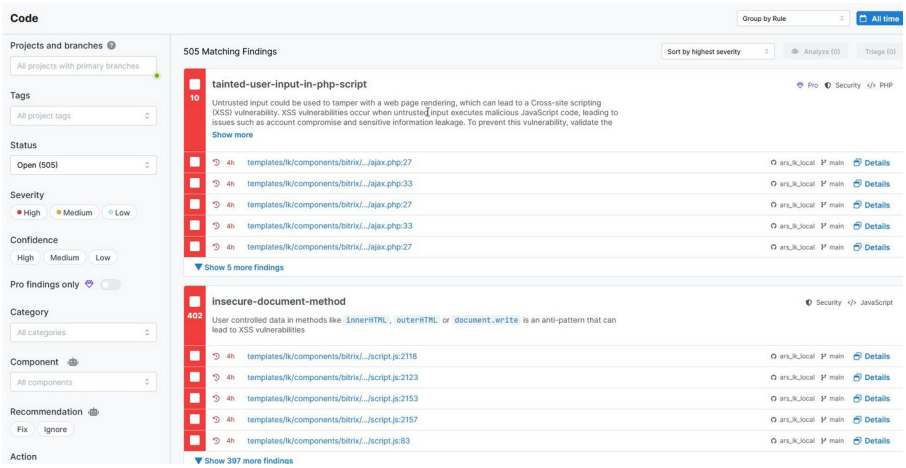


Рисунок 3 - Уязвимости в PHP-коде и JavaScript
DOI: https://doi.org/10.60797/IRJ.2025.155.1.5

Примечание: лист 1

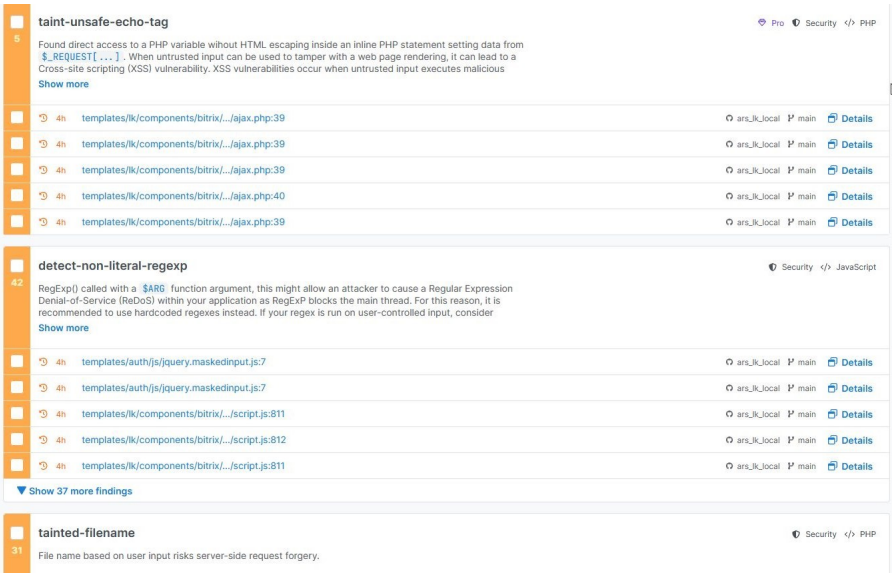


Рисунок 4 - Уязвимости в PHP-коде и JavaScript
DOI: https://doi.org/10.60797/IRJ.2025.155.1.6

Примечание: лист 2

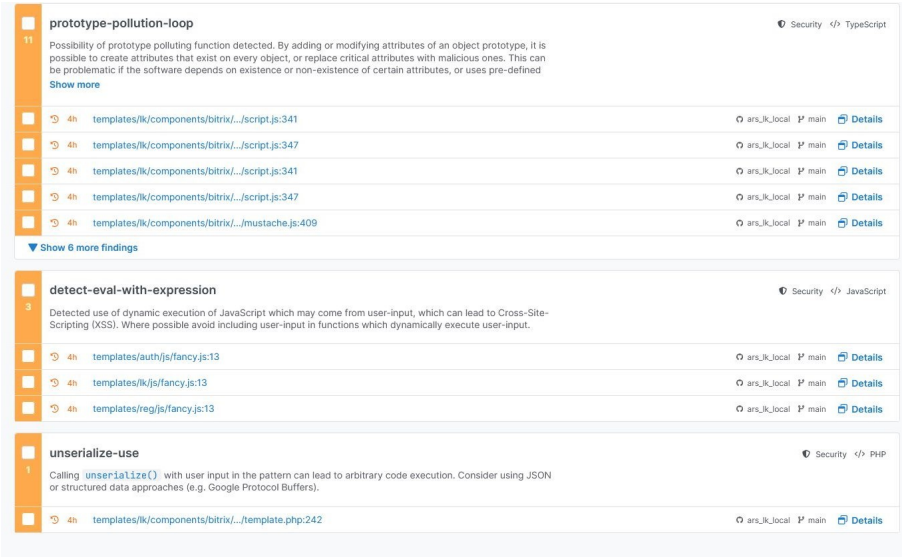


Рисунок 5 - Уязвимости в PHP-коде и JavaScript
DOI: https://doi.org/10.60797/IRJ.2025.155.1.7

Примечание: лист 3

7.2 Выводы и рекомендации по результатам тестирования

В процессе анализа были выявлены уязвимости, которые могут подвергнуть веб-приложение test.missoff.ru угрозам при взаимодействии с пользователями. Следует отметить, что тестирование проводилось с отключенными защитными модулями «1С-Битрикс», такими как проактивный фильтр и встроенный антивирус. Дополнительные тесты с включенными средствами защиты не изменили обнаруженные результаты, что указывает на устойчивость выявленных уязвимостей к штатным защитным механизмам платформы.

Особое внимание следует обратить на используемую версию языка программирования PHP — 7.4. В текущей версии PHP веб-приложения на платформе «1С-Битрикс» демонстрируют повышенную уязвимость. Рекомендуется обновить версию PHP до 8.2 или выше, что обеспечит не только повышение уровня безопасности, но и улучшение производительности. Поддержка актуальных версий PHP помогает устранить множество известных уязвимостей и способствует совместимости с новыми функциями безопасности.

Также выявлены следующие аспекты, требующие внимания:

1. Необходимость удаления базовых шаблонов и тестовых модулей. Шаблоны и модули, установленные по умолчанию, представляют потенциальную угрозу, так как их структура и стандартные настройки широко известны и могут быть использованы злоумышленниками. Удаление таких компонентов, а также ограничение доступа к неиспользуемым функциям поможет снизить риск несанкционированного доступа.

2. Проблемы форм обратной связи. Часто подобные формы являются целью атак, особенно в случае отсутствия надлежащей защиты от CSRF и XSS уязвимостей. Рекомендуется дополнительно проверить все формы на предмет корректного внедрения CSRF-токенов и политик CSP, а также обеспечить их соответствие актуальным требованиям OWASP.

В результате, для улучшения защищенности веб-приложения настоятельно рекомендуется внедрение следующих мер:

· Актуализация серверного ПО до последних безопасных версий.

· Удаление всех ненужных тестовых и демонстрационных компонентов.

· Оптимизация конфигураций безопасности с учетом рекомендаций, предоставленных в отчете, для защиты от атак типа SQL-инъекций, XSS и CSRF.

Принятие указанных мер повысит общий уровень безопасности и минимизирует возможные риски эксплуатации веб-приложения.

На последнем этапе, по результатам тестирования составляются отчеты, ПМИ и протокол испытаний. В заключении проведенных работ по аудиту приложений по «Общим критериям» Оценщик пишет «Технический отчет», где фиксируется выполнение всех шагов оценки на ОУД-4 по ГОСТ [4].

Заключение

В данной статье рассмотрена методология оценки безопасности мобильных и веб-приложений финансового сектора по «Общим критериям» [2]. Цели научной работы достигнуты. Для достижения первой цели исследования был проведен тщательный обзор литературы по теории и практике «Общих критериев». Необходимо отметить недостаточность научных трудов по данной проблеме, по причине ограничений конфиденциальности такого рода работ, особенно в банковской сфере. Однако, благодаря обзору литературы удалось изучить проблематику в теоретическом плане и сделать обоснованный выбор методологии оценки безопасности приложений в пользу «Общих критериев».

Для достижения второй цели научной работы был описан алгоритм тестирования процедур ATE_FUN, ATE_IND и AVA_VAN по ГОСТ [4] и апробирован автором для практического применения.

В рамках работы по третьей цели статьи был проведен инструментальный анализ сайта test.missoff.ru по методологии «Общих критериев» на уязвимости и показано, как проводятся на практике и документируются подобные работы.

Научная новизна данной статьи заключается в адаптации методологии «Общих критериев» для практической проверки приложений финансового сектора на уязвимости. В работе проведен эксперимент с тестированием веб-приложения по этой методологии, в результате которого показана эффективность методики «Общих критериев» и ее применимость на практике.

Автор приходит к выводу, что для повышения уровня безопасности мобильных и веб-приложений финансового сектора необходимо периодически проверять приложения по ОУД-4. А наиболее лучшим вариантом является организация процессов безопасной разработки ПО в компании.

Конфликт интересов

Не указан.

Рецензия

Артамонов В.А., Международная академия информационных технологий (МНОО "МАИТ), Минск Беларусь
DOI: https://doi.org/10.60797/IRJ.2025.155.1.8

Conflict of Interest

None declared.

Review

Артамонов V.A., International Academy of information technologies, Minsk Belarus
DOI: https://doi.org/10.60797/IRJ.2025.155.1.8

Список литературы / References

1. Милаков А.С. Методология оценки финансовых мобильных и веб-приложений на основе «Общих критериев» / А.С. Милаков // Международный научно-исследовательский журнал. — 2024. — №8 (146). — URL: https://research-journal.org/archive/8-146-2024-august/10.60797/IRJ.2024.146.149 (дата обращения: 02.10.2024). — DOI: 10.60797/IRJ.2024.146.149

2. Common Criteria for Information Technology Security Evaluation (CC). — URL: https://www.commoncriteriaportal.org/index.cfm (accessed: 02.10.2024).

3. Путято М.М. Сравнительный анализ существующих методик исследования защищенности мобильных приложений / М.М. Путято, А.С. Макарян, М.А. Карманов [и др.] // Прикаспийский журнал: управление и высокие технологии. — 2022. — № 4 (60). — URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-suschestvuyuschih-metodik-issledovaniya-zaschischennosti-mobilnyh-prilozheniy (дата обращения: 02.10.2024).

4. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

5. Барабанов А.В. Разработка типовой методики анализа уязвимостей в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации / А.В. Барабанов, А.В. Федичев // Вопросы кибербезопасности. — 2016. — № 2 (15). — URL: https://cyberleninka.ru/article/n/razrabotka-tipovoy-metodiki-analiza-uyazvimostey-v-veb-prilozheniyah-pri-provedenii-sertifikatsionnyh-ispytaniy-po-trebovaniyam (дата обращения: 02.10.2024).

6. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

7. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».

8. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

9. Методический документ «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций». — Банк России, 2021.

10. Kara M. Review on common criteria as a secure software development model / M. Kara // International Journal of Computer Science and Information Technology. — 2012 — № 4 (2). — P. 83–94. — DOI: 10.5121/IJCSIT.2012.4207.

11. Aven T. A unified framework for risk and vulnerability analysis covering both safety and security / T. Aven // IEEE Engineering Management Review. — 2011 — № 39 (4). — P. 123–134. — DOI: 10.1109/EMR.2011.6093894.

12. Mell P. Improving the Common Vulnerability Scoring System / P. Mell, K.A. Scarfone // Iet Information Security. — 2007. — № 1 (3). — P. 119–127. — DOI: 10.1049/IET-IFS:20060055.

13. Артамонов В.А. Безопасность проектирования программного обеспечения / В.А. Артамонов, Е.В. Артамонова, А.С. Милаков. — Санкт-Петербург : Афина, 2024.

14. Оценочный уровень доверия (ОУД4) и ГОСТ Р ИСО/МЭК 15408-3-2013. Введение. — URL: https://habr.com/ru/companies/swordfish_security/articles/543016/ (дата обращения: 02.10.2024).

15. Оценочный уровень доверия (ОУД4) и ГОСТ Р ИСО/МЭК 15408-3-2013. Разработчик. — URL: https://habr.com/ru/companies/swordfish_security/articles/569576/ (дата обращения: 02.10.2024).

16. Оценочный уровень доверия (ОУД4) и ГОСТ Р ИСО/МЭК 15408-3-2013. Оценщик. — URL: https://habr.com/ru/companies/swordfish_security/articles/750590/ (дата обращения: 02.10.2024).

17. Безопасность API веб-приложений. — URL: https://habr.com/ru/companies/swordfish_security/articles/780308/ (дата обращения: 02.10.2024).

Список литературы на английском языке / References in English

1. Milakov A.S. Metodologija ocenki finansovyh mobil'nyh i veb-prilozhenij na osnove «Obshhih kriteriev» [Methodology of evaluation of financial mobile and web applications on the basis of ‘Common Criteria’] / A.S. Milakov // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Research Journal]. — 2024. — №8 (146). — URL: https://research-journal.org/archive/8-146-2024-august/10.60797/IRJ.2024.146.149 (accessed: 02.10.2024). — DOI: 10.60797/IRJ.2024.146.149 [in Russian]

2. Common Criteria for Information Technology Security Evaluation (CC). — URL: https://www.commoncriteriaportal.org/index.cfm (accessed: 02.10.2024).

3. Putjato M.M. Sravnitel'nyj analiz sushhestvujushhih metodik issledovanija zashhishhennosti mobil'nyh prilozhenij [Comparative analysis of existing methods of mobile applications security research] / M.M. Putjato, A.S. Makarjan, M.A. Karmanov [i dr.] // Prikaspijskij zhurnal: upravlenie i vysokie tehnologii [Caspian Journal: Management and High Technologies]. — 2022. — № 4 (60). — URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-suschestvuyuschih-metodik-issledovaniya-zaschischennosti-mobilnyh-prilozheniy (accessed: 02.10.2024). [in Russian]

4. GOST R ISO/MJeK 18045-2013 «Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Metodologija ocenki bezopasnosti informacionnyh tehnologij» [GOST R ISO/IEC 18045-2013 ‘Information technology. Methods and means of ensuring security. Information technology security assessment methodology’]. [in Russian]

5. Barabanov A.V. Razrabotka tipovoj metodiki analiza ujazvimostej v veb-prilozhenijah pri provedenii sertifikacionnyh ispytanij po trebovanijam bezopasnosti informacii [Development of a standard methodology for analysing vulnerabilities in web applications during certification tests on information security requirements] / A.V. Barabanov, A.V. Fedichev // Voprosy kiberbezopasnosti [Cyber Security Issues]. — 2016. — № 2 (15). — URL: https://cyberleninka.ru/article/n/razrabotka-tipovoy-metodiki-analiza-uyazvimostey-v-veb-prilozheniyah-pri-provedenii-sertifikatsionnyh-ispytaniy-po-trebovaniyam (accessed: 02.10.2024). [in Russian]

6. GOST R ISO/MJeK 15408-1-2012 «Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 1. Vvedenie i obshhaja model'» [GOST R ISO/IEC 15408-1-2012 ‘Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technology. Part 1. Introduction and general model’]. [in Russian]

7. GOST R ISO/MJeK 15408-2-2013 «Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 2. Funkcional'nye komponenty bezopasnosti» [GOST R ISO/IEC 15408-2-2013 ‘Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technology. Part 2. Functional components of security’]. [in Russian]

8. GOST R ISO/MJeK 15408-3-2013 «Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 3. Komponenty doverija k bezopasnosti» [GOST R ISO/IEC 15408-3-2013 ‘Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technology. Part 3. Security trust components’]. [in Russian]

9. Metodicheskij dokument «Profil' zashhity prikladnogo programmnogo obespechenija avtomatizirovannyh sistem i prilozhenij kreditnyh organizacij i nekreditnyh finansovyh organizacij» [Methodological Document ‘Protection Profile of Application Software of Automated Systems and Applications of Credit Organisations and Non-Credit Financial Organisations’]. — Bank of Russia, 2021. [in Russian]

10. Kara M. Review on common criteria as a secure software development model / M. Kara // International Journal of Computer Science and Information Technology. — 2012 — № 4 (2). — P. 83–94. — DOI: 10.5121/IJCSIT.2012.4207.

11. Aven T. A unified framework for risk and vulnerability analysis covering both safety and security / T. Aven // IEEE Engineering Management Review. — 2011 — № 39 (4). — P. 123–134. — DOI: 10.1109/EMR.2011.6093894.

12. Mell P. Improving the Common Vulnerability Scoring System / P. Mell, K.A. Scarfone // Iet Information Security. — 2007. — № 1 (3). — P. 119–127. — DOI: 10.1049/IET-IFS:20060055.

13. Artamonov V.A. Bezopasnost' proektirovanija programmnogo obespechenija [Software design security] / V.A. Artamonov, E.V. Artamonova, A.S. Milakov. — St.Petersburg : Afina, 2024. [in Russian]

14. Ocenochnyj uroven' doverija (OUD4) i GOST R ISO/MJeK 15408-3-2013. Vvedenie [Estimated confidence level (EIQ4) and GOST R ISO/IEC 15408-3-2013. Introduction]. — URL: https://habr.com/ru/companies/swordfish_security/articles/543016/ (accessed: 02.10.2024). [in Russian]

15. Ocenochnyj uroven' doverija (OUD4) i GOST R ISO/MJeK 15408-3-2013. Razrabotchik [Estimated Confidence Level (ECL4) and GOST R ISO/IEC 15408-3-2013. Developer]. — URL: https://habr.com/ru/companies/swordfish_security/articles/569576/ (accessed: 02.10.2024). [in Russian]

16. Ocenochnyj uroven' doverija (OUD4) i GOST R ISO/MJeK 15408-3-2013. Ocenshhik [Estimated confidence level (EIQ4) and GOST R ISO/IEC 15408-3-2013. Evaluator]. — URL: https://habr.com/ru/companies/swordfish_security/articles/750590/ (accessed: 02.10.2024). [in Russian]

17. Bezopasnost' API veb-prilozhenij [Web application API security]. — URL: https://habr.com/ru/companies/swordfish_security/articles/780308/ (accessed: 02.10.2024). [in Russian]