

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

DOI: <https://doi.org/10.60797/IRJ.2024.146.149>

МЕТОДОЛОГИЯ ОЦЕНКИ ФИНАНСОВЫХ 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 организаций финансовой сферы. Автор ставит проблему нарушений безопасности подобных приложений. Решение проблемы – в периодической оценке уязвимостей финансовых приложений. В статье приводится обзор наиболее распространенных методологий оценки приложений финансовой сферы: OWASP, NIST, ГОСТ Р ИСО/МЭК 18045-2013. Автор выделяет методологию оценки финансовых мобильных и веб-приложений на основе «Общих критериев», как наиболее актуальную в Российской Федерации и других странах. В работе рассматривается практика оценки приложений на оценочный уровень доверия. В статье детально описывается процесс разработки «Задания по безопасности» (ЗБ) – базового документа для оценки приложений на проблемы информационной безопасности.

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

A METHODOLOGY FOR EVALUATING FINANCIAL MOBILE AND WEB APPLICATIONS 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 of financial organizations. The author raises the issue of security breaches of such applications. The solution lies in periodic vulnerability evaluation of financial applications. The paper provides an overview of the most common methodologies for assessing financial applications: OWASP, NIST, GOST R ISO/IEC 18045-2013. The author singles out the methodology of evaluation of financial mobile and web applications based on "Common criteria" as the most relevant in the Russian Federation and other countries. The work discusses the practice of evaluating applications for the estimated level of trust. The paper provides a detailed description of the process of developing a "Security Assignment" (SA) – a basic document for assessing applications for information security issues.

Keywords: mobile applications, web applications, banks, financial organizations, vulnerabilities, threats, threat model, evaluated confidence level, common criteria.

Введение

В последние годы наблюдается стремительный рост использования мобильных и веб-приложений в банковской и финансовой сферах. Это обусловлено удобством и доступностью таких сервисов для пользователей. Однако вместе с ростом популярности увеличиваются и риски, связанные с уязвимостями этих приложений. По данным различных исследований, значительное количество мобильных и веб-приложений содержат критические уязвимости, которые могут быть использованы злоумышленниками для проведения атак. Например, по данным исследования «Стингрей Технолджиз» [1] около 56% мобильных приложений российских разработчиков имеют уязвимости высокой и наивысшей степени критичности, которые могут привести к утечке данных пользователей или финансовым потерям. В 2023 году главной угрозой безопасности мобильных приложений остаются типичные уязвимости систем информационной безопасности (ИБ). К примеру, хранение конфиденциальной информации пользователя в открытом виде, хранение секретной информации, полученной от сторонних сервисов, а также их неправильная настройка, которая разрешает злоумышленнику получить доступ к расширенным функциям приложения, недоступным для обычного клиента. Еще одной важной проблемой является отсутствие проверки окружения, в котором запускается приложение.

Эти факторы приводят к тому, что мобильные и веб-приложения необходимо подвергать периодической проверке на наличие уязвимостей. Но в этом случае возникает вопрос: как выбрать методологию аудита мобильных и веб-приложений? Конечно же, в случае аудита обычных приложений можно просто периодически делать тестирование на проникновение или проверку исходного кода на уязвимости. Однако приложения финансовой сферы являются наиболее уязвимыми в плане атаки злоумышленников, так как они служат для операций с денежными средствами.

Данный фактор риска приводит к тому, что проблематика угроз ИБ встает в полный рост и необходимо выбрать методику, по которой будут регулярно тестироваться приложения финансового сектора.

Существует несколько методологий для оценки безопасности мобильных и веб-приложений, такие как OWASP, NIST, ISO/IEC 27001, а также стандарт [2].

В плане сравнительных характеристик для нас представляет интерес исследование [3], в котором авторы проводят детальное описание методологий ГОСТ Р ИСО/МЭК 18045-2013 [4] и стандарта OWASP MASVS [5], использующегося в совокупности с техническим руководством тестирования безопасности в аспекте мобильных устройств [6].

В научной статье [3] авторы довольно подробно рассматривают две методологии оценки мобильных приложений и делают выводы в пользу OWASP, выделяя несущественные недостатки методологии ГОСТ Р ИСО/МЭК 18045-2013. В результате, по мнению авторов работы [3], можно использовать обе методологии, они дают хорошие результаты в процессе проверки мобильных приложений.

Что касается оценки веб-приложений, то исследование [7] однозначно рекомендует ГОСТ Р ИСО/МЭК 18045-2013 — документ, содержащий методологию оценки, используемую при проведении испытаний по линии «Общих критериев».

«Общие критерии» в Российской Федерации опубликованы в виде национальных стандартов [8], [9], [10].

Стоит отметить, что при исследовании на уязвимости ИБ любых мобильных и веб-приложений (например, в сфере торговли, игр и развлечений и т.д.) специалисты могут выбрать любую из вышеперечисленных методологий. Однако, когда необходимо провести исследование на уязвимости мобильных и веб-приложений для финансового сектора, в РФ следует выполнять требования регулятора в этой сфере, а именно Банка России. Для того чтобы организовать процесс безопасной разработки и поддержки платежного ПО и пройти анализ уязвимостей приложения, требуемый положениями Банка России и отраслевым стандартом [11], [12], [13], [14], необходимо провести оценку соответствия на уровень доверия не ниже, чем ОУД-4 (оценочный уровень доверия). Также Банком России подготовлен профиль защиты (ПЗ) [15], который на данный момент носит рекомендательный характер.

Методика научных исследований

В статье применяются публикационный метод прогнозирования и методика экспертных оценок, а также опыт практических исследований уязвимостей мобильных и веб-приложений. Исследование проводилось следующим образом:

1. Изучение и анализ источников по тематике аудита мобильных и веб-приложений (монографии, научные статьи, международные и государственные стандарты, материалы из Интернета и т.д.).

2. Затем была решена проблема выбора методологии оценки мобильных и веб-приложений в финансовом секторе. Автором был выполнен анализ различных методик оценки финансовых приложений.

3. В итоге, выбор автора был сделан в пользу методологии оценки безопасности веб и мобильных приложений в финансовой сфере на базе «Общих критериев».

4. В работе приведена подробная методика анализа безопасности приложений на основе «Общих критериев».

5. Автор использовал практический опыт в области тестирования на безопасность мобильных и веб-приложений для обоснования своих научных исследований.

Цель работы:

1) обобщить литературные источники по оценке информационной безопасности мобильных и веб-приложений, а также сделать анализ нормативных документов в этой области;

2) кратко описать основные методологии оценки мобильных и веб-приложений и сделать обоснованный выбор в пользу методологии на базе «Общих критериев»;

3) выстроить алгоритм оценки мобильных и веб-приложений финансовой сферы по ОУД-4.

Оценка приложений финансовых структур по ОУД4

На данный момент в области разработки приложений популярен подход, который называется «безопасной разработкой программного обеспечения (ПО)» (англ. «Secure SDLC» или «Secure software development life cycle»). Если разработчики ПО других сфер деятельности могут выбрать совершенно любую методологию для «Secure SDLC», согласно исследованиям [16], то разработчики ПО для банковского сектора однозначно должны выбирать методику безопасной разработки по ОУД-4. Это обоснованно нормативными документами регуляторов, которые упоминались во Введении в статью.

Согласно нормативному документу [10] можно выделить этапы работ для оценки, которые указаны в таблице 1.

Таблица 1 - Обзор оценочных уровней доверия

DOI: <https://doi.org/10.60797/IRJ.2024.146.149.1>

Класс доверия	Семейств во доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Разработка	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_I				1	1	2	2

Класс доверия	Семейство	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
	MP							
	ADV_IN NT					2	3	3
	ADV_S PM						1	1
	ADV_T DS		1	2	3	4	5	6
Руководства	AGD_O PE	1	1	1	1	1	1	1
	AGD_P RE	1	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_C MC	1	2	3	4	4	5	5
	ALC_C MS	1	2	3	4	5	5	5
	ALC_D EL		1	1	1	1	1	1
	ALC_D VS			1	1	1	2	2
	ALC_FL R							
	ALC_L CD			1	1	1	1	2
	ALC_TA T				1	2	3	3
Оценка задания по безопасности	ASE_C CL		1	1	1	1	1	1
	ASE_EC D		1	1	1	1	1	1
	ASE_IN T		1	1	1	1	1	1
	ASE_O BJ		2	2	2	2	2	2
	ASE_RE Q		2	2	2	2	2	2
	ASE_SP D		1	1	1	1	1	1
	ASE_TS S	1	1	1	1	1	1	1
Тестирование	ATE_C OV		1	2	2	2	3	3
	ATE_DP T			1	2	3	3	4
	ATE_FU N		1	1	1	1	2	2
	ATE_IN D	1	2	2	2	2	2	3
Оценка уязвимостей	AVA_V AN	1	2	2	3	4	5	5

Далее необходимо определить ключевые роли, которые фигурируют в процессе оценивания по ОУД-4 [17]:

1. Заказчик (пользователь или владелец) – субъект, применяющий продукт (ПО) и требующий соответствие этого продукта определенным требованиям к ИБ.
2. Разработчик – субъект, который разрабатывает продукт и задает его жизненный цикл по требованиям Заказчика.
3. Оценщик – субъект, который проверяет соответствие разработанного ПО заданным требованиям.

В ходе работ по ОУД-4 необходимо:

- 1) разработать документацию, в которой задать функциональные требования к продукту и требования доверия;
- 2) практически применить заданные требования при разработке (или проверке) продукта;
- 3) выполнить тестирование приложений, оценку соответствия и анализ уязвимостей. Таким образом, на практике подтвердить, что заданные в документах требования к безопасности продукта выполняются.

Перечень работ и документации, выполняемых в ходе оценки по ОУД-4, приведен в таблице 2.

Таблица 2 - Перечень работ и документации, выполняемых в ходе оценки по ОУД-4

DOI: <https://doi.org/10.60797/IRJ.2024.146.149.2>

Класс доверия	Компонента доверия
ADV: Разработка	ADV_ARC.1 Описание архитектуры безопасности
	ADV_FSP.4 Полная функциональная спецификация
	ADV_IMP.1 Представление реализации ФБО
	ADV_TDS.3 Базовый модульный проект
AGD: Руководства	AGD_OPE.1 Руководство пользователя по эксплуатации
	AGD_PRE.1 Подготовительные процедуры
ALC: Поддержка жизненного цикла	ALC_CMC.4 Поддержка производства, процедуры приемки и автоматизации
	ALC.CMS.4 Охват УК отслеживания проблем
	ALC_DEL.1 Процедуры поставки
	ALC_DVS.1 Идентификация мер безопасности
	ALC_LCD.1 Определённая разработчиком модель жизненного цикла
	ALC_TAT.1 Полностью определённые инструментальные средства разработки
ASE: Оценка задания по безопасности	ASE_CCL.1 Утверждения о соответствии
	ASE_ECD.1 Определение расширенных компонентов
	ASE_INT.1 Введение ЗБ
	ASE_OBJ.2 Цели безопасности
	ASE_REQ.2 Производные требования безопасности
	ASE_SPD.1 Определение проблемы безопасности
	ASE_TSS.1 Краткая спецификация ОО
ATE: Тестирование	ATE_COV.2 Анализ покрытия
	ATE_DPT.2 Тестирование: модули обеспечения безопасности
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_VAN.3 Сосредоточенный анализ уязвимостей

На заключительном этапе Оценщик проводит оценку соответствия, выносит вердикт. Вердикт считается положительным, если все шаги оценки имеют положительный вердикт.

На рисунке 1 показана оценка достаточности и корректности выбранных мер защиты.

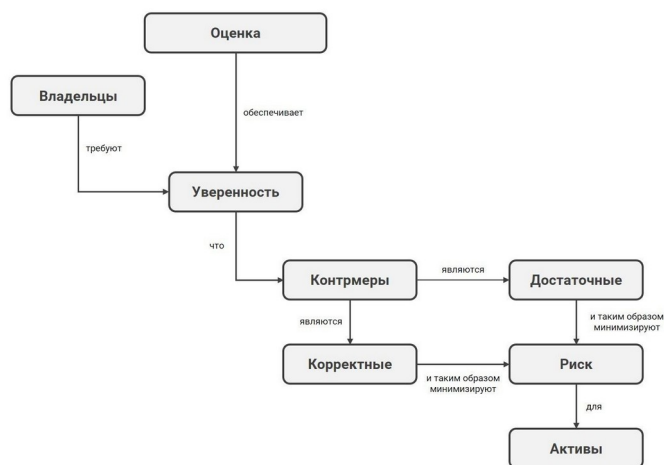


Рисунок 1 - Оценка достаточности и корректности выбранных мер защиты
DOI: <https://doi.org/10.60797/IRJ.2024.146.149.3>

Задание по безопасности — базовый документ в ОУД-4

Задание по безопасности (ЗБ, англ. Security Target) является основным документом в ОУД-4, фактически – это техническое задание, только в сфере ИБ. В первую очередь, при написании ЗБ следует определить объект оценки (ОО). Банковские системы, особенно в крупных банках, построены из тысячи модулей и интерфейсов. Если оценивать на безопасность все эти модули, то это будет очень трудоемкой работой. Поэтому выделяют наиболее значимые модули, которые отвечают за работу с клиентом и к ним имеется доступ из Интернета, к примеру, это могут быть системы дистанционного банковского обслуживания (ДБО) или личный кабинет (ЛК) пользователя. Дополнительно нужно оценивать интерфейсы к внешним системам, с которыми взаимодействует ОО, а также базы данных (БД) и системы журналирования.

После выделения ОО необходимо обследовать ОО и его окружение, выделить логические подсистемы и модули, определить интерфейсы и т.д.

На следующем этапе необходимо сформировать модель угроз. Для банковских приложений стоит воспользоваться моделью угроз, изложенной в документе [15]. Для приложений из нефинансовой сферы возможно подойдет моделирование угроз с сайта ФСТЭК [18]. Также необходимо определить угрозы для среды, в которой работает ОО.

Согласно работе [19] ЗБ – это абстрактный документ, который описывает реальные для банковского приложения угрозы и цели безопасности, в результате этого вырабатываются «Функциональные требования к безопасности» и «Требования доверия к безопасности».

Функциональные требования к безопасности – это требования к применяемым мерам безопасности, в соответствии с которыми надо разрабатывать систему.

Требования доверия к безопасности – это совокупность требований к оценке, в соответствии с которыми необходимо осуществлять внешний аудит.

Структура задания по безопасности приведена на рисунке 2.

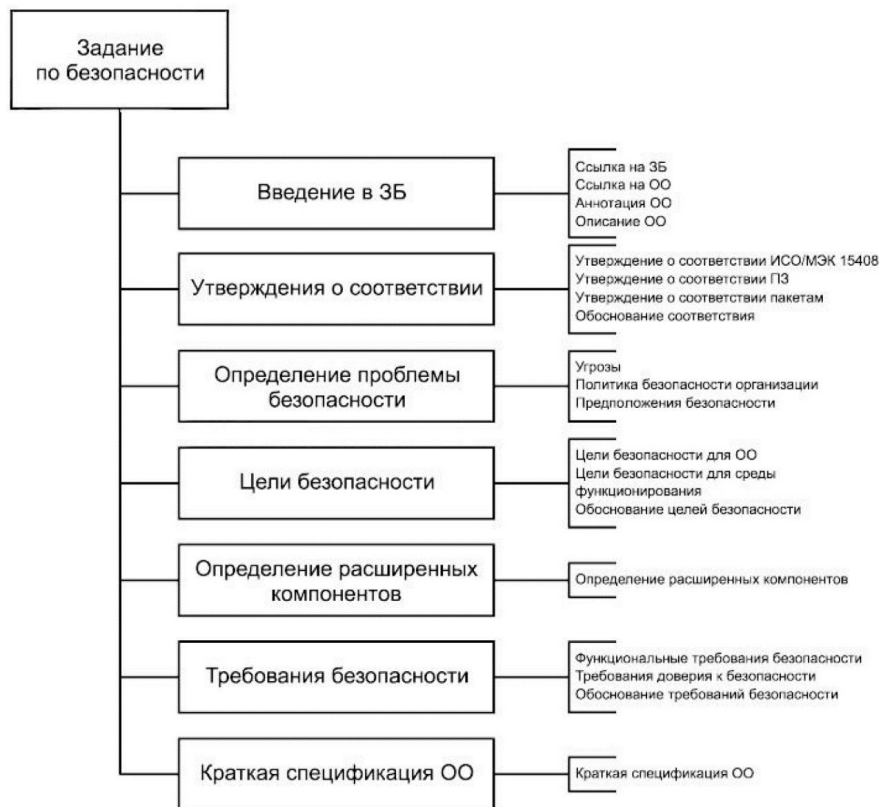


Рисунок 2 - Структура задания по безопасности
DOI: <https://doi.org/10.60797/IRJ.2024.146.149.4>

Разработчик должен отличать «Задание по безопасности» от другого подобного документа – «Профиля защиты» (ПЗ). Дело в том, что ЗБ разрабатывается на конкретную систему (например, для конкретного ДБО банка или ЛК некредитной организации), а ПЗ готовится на типовой элемент системы (к примеру, на межсетевой экран и т.д.).

Согласно [9] функциональные требования к безопасности образуют классы, далее классы декомпозируются в семейства и в итоге, компоненты являются наименьшим набором требований. Ниже перечислим классы функциональных требований к безопасности по [9]:

- FAU аудит безопасности;
- FCO связь;
- FCS криптографическая поддержка;
- FDP защита данных пользователя;
- FIA идентификация и аутентификация;
- FMT управление безопасностью;
- FPR приватность работы в системе;
- FPT защита функций безопасности объекта оценки или надежность средств защиты;
- FRU контроль за использованием ресурсов;
- FTA контроль доступа к системе;
- FTR доверенный путь/ канал.

На рисунке 3 показано как декомпозируется класс [9].

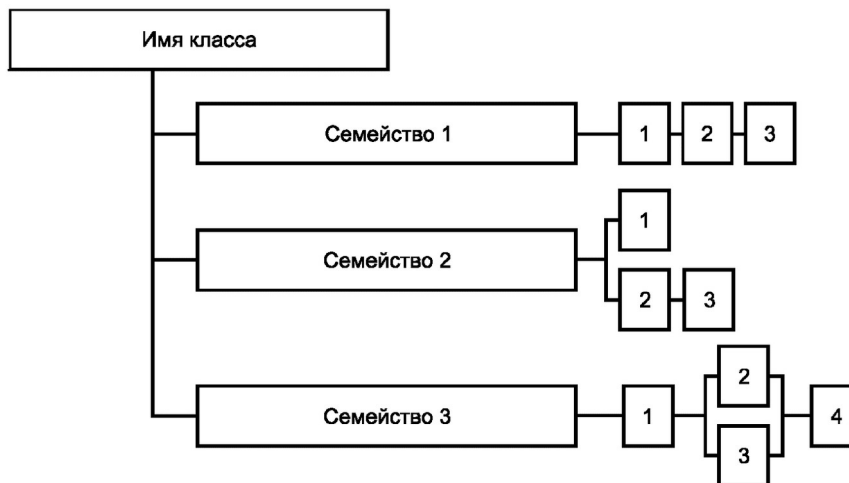


Рисунок 3 - Пример декомпозиции класса
DOI: <https://doi.org/10.60797/IRJ.2024.146.149.5>

В качестве примера попробуем декомпозировать класс FAU Аудит безопасности (см. рис. 4 [9]).

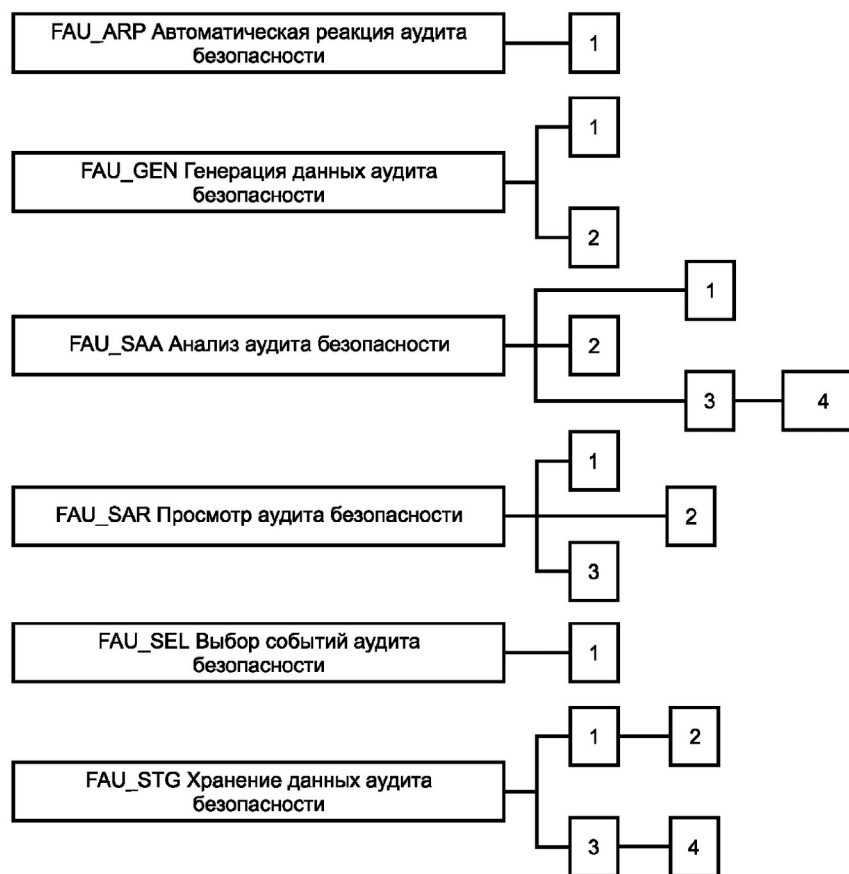


Рисунок 4 - Пример декомпозиции класса FAU
DOI: <https://doi.org/10.60797/IRJ.2024.146.149.6>

Требования доверия показаны в таблице 1. Требования доверия привязаны к ролям (некоторые требования должен выполнить Разработчик, а некоторые – Оценщик).

Тестирование и анализ уязвимостей

После разработки «Задания по безопасности» и других документов по ОУД-4 стоит перейти к практической части, а именно – к тестированию приложения и анализу уязвимостей.

Класс «Тестирование» (ATE) включает в себя четыре семейства:

- ATE_COV «Покрытие»;
- ATE_DPT «Глубина»;

- ATE_FUN «Функциональное тестирование»;
- ATE_IND «Независимое тестирование».

Тестирование представляет доверие к тому моменту, что ФБО (функции безопасности ОО) функционируют в описанном в документации режиме. На рисунке 5 показан процесс декомпозиции класса АТЕ.



Рисунок 5 - Декомпозиция класса АТЕ
DOI: <https://doi.org/10.60797/IRJ.2024.146.149.7>

ATE_FUN «Функциональное тестирование» выполняется и документируется разработчиком. ATE_IND «Независимое тестирование» проводится оценщиком.

Класс AVA «Оценка уязвимостей» предназначен для нахождения пригодных для использования уязвимостей, которые были внесены при разработке или при эксплуатации ОО. Анализ уязвимостей – это оценка факторов эксплуатации потенциальных уязвимостей, выявленных в процессе оценки разработки и функционирования ОО или другими методами (например, путем количественного или статистического анализа режима функционирования механизмов безопасности), позволить злоумышленникам нарушить функциональные требования безопасности.

Анализ уязвимостей позволяет детально рассмотреть угрозы эксплуатации злоумышленником уязвимостей, которые могут позволить нарушителю выполнить несанкционированный доступ к данным, нарушить выполнение функций безопасности объекта оценки (ФБО), внести изменения в ФБО или ограничить права других пользователей.

Чтобы провести анализ уязвимостей инженеры используют автоматизированные инструменты, такие как статические и динамические анализаторы кода, фреймворки для тестирования на проникновение, а также специализированные сканеры уязвимостей.

Одним из наиболее часто используемых инструментов является OWASP ZAP (Zed Attack Proxy), который позволяет проводить динамический анализ безопасности веб-приложений. Для мобильных приложений используется MobSF (Mobile Security Framework), который предоставляет возможности для статического и динамического анализа.

Заключение

По итогам проведенного исследования была выбрана методология оценки безопасности финансовых мобильных и веб-приложений на основе «Общих критериев». Данная методология позволяет проводить всесторонний анализ безопасности приложений, выявлять и устранять уязвимости, что значительно повышает уровень защиты финансовых данных пользователей. Также данная методология полностью укладывается в требования регуляторов и соответствует нормативным документам Банка России.

Проведенное исследование демонстрирует важность применения методологии оценки безопасности мобильных и веб-приложений финансовых организаций на основе «Общих критериев».

Стоит отметить ограниченность изученных автором источников ([3], [7] и других аналогичных статей). Дело в том, что по тематике методологий оценки мобильных и веб-приложений (особенно финансовой сферы) не так много научных статей, потому что работы по оценке на ОУД-4 лицензируемы и строго регулируются соответствующими государственными институтами, а также на результаты этих работ накладываются ограничения по коммерческой тайне или соглашению о неразглашении. Это усложняет научным работникам изучение подобных методологий на практике. К примеру, работа [3] только проводит сравнение методологий ГОСТ Р ИСО/МЭК 18045-2013 [4] и стандарта OWASP MASVS, а статья [7] ограничена только оценкой веб-приложений.

Научная новизна работы заключается:

- 1) в применении комплексного подхода к оценке безопасности, что позволяет учитывать различные аспекты и угрозы, присущие современным финансовым приложениям;
- 2) в построении грамотной методологии по ГОСТ Р ИСО/МЭК 18045-2013 [4] для оценки веб и мобильных приложений финансового сектора на ОУД-4;

3) в разработке алгоритма оценки на ОУД-4 для приложений финансового сектора, который согласуется с нормативными документами регулятора и применим на практике.

В результате применения этого исследования значительно повышается уровень защиты данных и доверие пользователей к финансовым услугам, предоставляемым через мобильные и веб-приложения.

Конфликт интересов

Не указан.

Рецензия

Белашова Е.С., Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань Российская Федерация
DOI: <https://doi.org/10.60797/IRJ.2024.146.149.8>

Conflict of Interest

None declared.

Review

Belashova E.S., Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan Russian Federation
DOI: <https://doi.org/10.60797/IRJ.2024.146.149.8>

Список литературы / References

1. Оценка защищённости мобильных приложений. Ежегодное исследование «Стингрей Технолоджиз» // Стингрей. — URL: <https://mobile-stingray.ru/research/security-analysis> (дата обращения: 21.06.2024).
2. Common Criteria for Information Technology Security Evaluation (CC). — URL: <https://www.commoncriteriaportal.org/index.cfm> (accessed: 21.06.2024).
3. Путьто М. М. Сравнительный анализ существующих методик исследования защищённости мобильных приложений / М. М. Путьто, А. С. Макарян и др. // Прикаспийский журнал: управление и высокие технологии. — 2022. — № 4(60). — URL: <https://cyberleninka.ru/article/n/sravnitelnyy-analiz-suschestvuyuschih-metodik-issledovaniya-zaschischnosti-mobilnyh-prilozheniy> (дата обращения: 21.06.2024).
4. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий». — Введ. 2014–07–01.
5. OWASP Mobile Application Security Verification Standard (MASVS) v2.1.0. — URL: <https://mas.owasp.org/MASVS> (accessed: 21.06.2024).
6. OWASP Mobile Application Security Testing Guide (MASTG) v1.7.0. — URL: <https://mas.owasp.org/MASTG> (accessed: 21.06.2024).
7. 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).
8. 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». — Введ. 2013–12–01.
9. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности». — Введ. 2014–09–01.
10. 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». — Введ. 2014–09–01.
11. Положение Банка России № 672-П «О требованиях к защите информации в платежной системе Банка России». — URL: <https://www.garant.ru/products/ipo/prime/doc/72104924/> (дата обращения: 21.06.2024).
12. Положение Банка России от 17 апреля 2019 г. N 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента». — URL: <https://www.garant.ru/products/ipo/prime/doc/72146408/> (дата обращения: 21.06.2024).
13. Положение Банка России от 4 июня 2020 г. № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». — URL: <https://www.garant.ru/products/ipo/prime/doc/74609682/> (дата обращения: 21.06.2024).
14. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер». — Введ. 2018–01–01.
15. Методический документ «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций». — Банк России, 2020. — 155 с.
16. Артамонов В. А. Безопасность проектирования программного обеспечения / В. А. Артамонов, Е. В. Артамонова, А. С. Милаков. — СПб. : ООО «ИД «Афина». — 2024.
17. 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: 21.06.2024).
18. Банк данных угроз безопасности информации, Федеральная служба по техническому и экспортному контролю (ФСТЭК России). — URL: <https://bdu.fstec.ru/threat-section/shaper-threats> (дата обращения: 21.06.2024).
19. 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: 21.06.2024).

Список литературы на английском языке / References in English

1. Ocenka zashhishhjonnosti mobil'nyh prilozhenij. Ezhegodnoe issledovanie «Stingrej Tehnologdzhiz» [Assessment of the security of mobile applications. Annual research of Stingray Technologies] // Stingrej [Stingray]. — URL: <https://mobile-stingray.ru/research/security-analysis> (accessed: 21.06.2024). [in Russia]
2. Common Criteria for Information Technology Security Evaluation (CC). — URL: <https://www.commoncriteriaportal.org/index.cfm> (accessed: 21.06.2024).
3. Putyato M. M. Sravnitel'nyj analiz sushhestvujushhijh metodik issledovaniya zashhishhennosti mobil'nyh prilozhenij [Comparative analysis of existing methods for researching the security of mobile applications] / M. M. Putyato, A. S. Makaryan [et al.] // 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: 21.06.2024). [in Russia]
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. Methodology of information technology security assessment"]. — Introd. 2014–07–01. [in Russia]
5. OWASP Mobile Application Security Verification Standard (MASVS) v2.1.0. — URL: <https://mas.owasp.org/MASVS> (accessed: 21.06.2024).
6. OWASP Mobile Application Security Testing Guide (MASTG) v1.7.0. — URL: <https://mas.owasp.org/MASTG> (accessed: 21.06.2024).
7. Barabanov A. V. Razrabotka tipovoj metodiki analiza ujazvimostej v veb-prilozhenijah pri provedenii sertifikacionnyh ispytanj po trebovanijam bezopasnosti informacii [Development of a standard methodology for analyzing vulnerabilities in web applications during certification tests for information security requirements] / A. V. Barabanov, A. V. Fedichev // Voprosy kiberbezopasnosti [Issues of cybersecurity]. — 2016. — № 2(15). [in Russia]
8. 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 evaluating information technology security. Part 1. Introduction and general model"]. — Introd. 2013–12–01. [in Russia]
9. 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 evaluating information technology security. Part 2. Functional safety components"]. — Introd. 2014–09–01. [in Russia]
10. 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 evaluating information technology security. Part 3. Components of trust in security"]. — Introd. 2014–09–01. [in Russia]
11. Polozhenie Banka Rossii № 672-P «O trebovanijah k zashhite informacii v platezhnoj sisteme Banka Rossii» [Regulation of the Bank of Russia No. 672-P "On requirements for the protection of information in the payment system of the Bank of Russia"]. — URL: <https://www.garant.ru/products/ipo/prime/doc/72104924/> (accessed: 21.06.2024). [in Russia]
12. Polozhenie Banka Rossii ot 17 aprelja 2019 g. N 683-P «Ob ustanovlenii objazatel'nyh dlja kreditnyh organizacij trebovanij k obespecheniju zashhity informacii pri osushhestvlenii bankovskoj dejatel'nosti v celjah protivodejstvija osushhestvleniju perevodov denezhnyh sredstv bez soglasija klienta» [Regulation of the Bank of Russia dated April 17, 2019 No. 683-P "On the establishment of mandatory requirements for credit institutions to ensure the protection of information in banking activities in order to counteract the transfer of funds without the consent of the client"]. — URL: <https://www.garant.ru/products/ipo/prime/doc/72146408/> (accessed: 21.06.2024). [in Russia]
13. Polozhenie Banka Rossii ot 4 ijunya 2020 g. № 719-P «O trebovanijah k obespecheniju zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv i o porjadke osushhestvlenija Bankom Rossii kontrolja za sobljudeniem trebovanij k obespecheniju zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv» [Regulation of the Bank of Russia dated June 4, 2020 No. 719-P "On the Requirements for Ensuring Information Protection when Making Money Transfers and on the Procedure for the Bank of Russia to monitor compliance with the requirements for ensuring information protection when making money transfers"]. — URL: <https://www.garant.ru/products/ipo/prime/doc/74609682/> (accessed: 21.06.2024). [in Russia]
14. GOST R 57580.1-2017 «Bezopasnost' finansovyh (bankovskih) operacij. Zashhita informacii finansovyh organizacij. Bazovyj sostav organizacionnyh i tehniceskikh mer» [GOST R 57580.1-2017 "Security of financial (banking) transactions. Protection of information of financial organizations. The basic composition of organizational and technical measures"]. — Introd. 2018–01–01. [in Russia]
15. Metodicheskij dokument «Profil' zashhity prikladnogo programmnoho obespechenija avtomatizirovannyh sistem i prilozhenij kreditnyh organizacij i nekreditnyh finansovyh organizacij» [Methodological document "Profile of protection of application software of automated systems and applications of credit institutions and non-credit financial organizations"]. — Bank of Russia, 2020. — 155 p. [in Russia]
16. Artamonov V. A. Bezopasnost' proektirovaniya programmnoho obespechenija [Software design security] / V. A. Artamonov, E. V. Artamonova, A. S. Milakov. — St. Petersburg : LLC "ID "Athena". — 2024. [in Russia]
17. Ocenochnyj uroven' doverija (OUD4) i GOST R ISO/MJeK 15408-3-2013. Vvedenie [The estimated level of trust (OUD4) and GOST R ISO/IEC 15408-3-2013. Introduction]. — URL: https://habr.com/ru/companies/swordfish_security/articles/543016/ (accessed: 21.06.2024). [in Russia]

18. Bank dannyh ugroz bezopasnosti informacii, Federal'naja sluzhba po tehničeskomu i jeksportnomu kontrolju (FSTJeK Rossii) [The database of information security threats, the Federal Service for Technical and Export Control (FSTEC of Russia)]. — URL: <https://bdu.fstec.ru/threat-section/shaper-threats> (accessed: 21.06.2024). [in Russia]
19. Ocenочnyj uroven' doverija (OUD4) i GOST R ISO/MJeK 15408-3-2013. Razrobotchik [The estimated level of trust (OUD4) and GOST R ISO/IEC 15408-3-2013. Developer]. — URL: https://habr.com/ru/companies/swordfish_security/articles/569576/ (accessed: 21.06.2024). [in Russia]