СТИНГРЕЙ

Аналитическая записка

По исследованиям компаний Стингрей Технолоджиз и Positive Technologies каждое третье мобильное приложение содержит хотя бы одну уязвимость высокого или критического уровня. При этом, скорость разработки очень высока. Согласно статистике Google Play в магазин приложений ежемесячно загружается около 10 тысяч новых приложений (по усредненным ежемесячным данным за 2022 год). Соответственно, с каждым годом уязвимых приложений, которыми активно пользуются как бизнес, так и частные клиенты, становится кратно больше.

Разработка мобильных приложений имеет свои особенности относительно классического цикла разработки Web-приложений - более быструю динамику разработки и процесс тестирования. Скорость выхода новых версий, дефицит специалистов по кибербезопасности на рынке и сложность тестирования (часть анализа защищенности выполняется вручную) порождают проблему роста числа уязвимостей в новых версиях приложений и невозможности в полном объеме протестировать каждую новую версию.

Одновременно, существует проблема скорости подготовки достойных экспертов, так как область кибербезопасности – достаточно сложная и требует значительных временных затрат на освоение. Многие учебные материалы для более продвинутых специалистов устаревают быстрее, чем человек успевает пройти необходимый тренинг. За 2022 год в мире было зафиксировано появление более 40 тысяч новых уязвимостей в мобильных приложениях. Это примерно 110 новых уязвимостей в день – рекорд за последние 7 лет.

Компании-лидеры рынка кибербезопасности (Стингрей, MobSF (OpenSource), RMS (OpenSource) – в России, и зарубежные, не предоставляющие свои услуги на территории РФ: NowSecure, AppKnox, Quixxi, ImmuniWeb, Pradeo, Ostorlab, HCL AppScan Mobile) разработали решения, совмещающие различные практики для проведения анализа защищенности продукта. В целях составления объективной картины ситуации на рынке решений для анализа защищенности и выявления конкурентных преимуществ Стингрей было проведено исследование и составлена сравнительная таблица по ключевым характеристикам всех существующих продуктов. Каждому критерию был присвоен вес: 10 – критическое требование, веса от 1 до 5 присвоены в зависимости от важности пункта и наличия функциональных альтернатив. Веса вычислялись по функции «мода» исходя из пожеланий заказчиков. В рамках составления сравнительного анализа были проведены пилотные проекты в 2022 году с каждым из продуктов, где оценивались их функциональные характеристики по каждому из критериев.

По результатам сравнительного анализа продукт Стингрей набрал 72 балла из 100 возможных. Это максимальный результат среди всех продуктов. Соответственно, Стингрей является оптимальным продуктом для решения задачи анализа защищенности мобильных приложений и вышеперечисленных проблем и существенно опережает конкурентов по функционалу и эксплуатационным возможностям, а также наиболее соответствует требованиям заказчиков и Регулятора.

СТИНГРЕЙ

Перечень используемых терминов и сокращений

Термин / Сокращение	Описание
Open source	Open Source проект – это десктопная, мобильная программа или веб-приложение с открытым исходным кодом. Разработчик приложения распространяет свой проект по бесплатной открытой лицензии. Каждый желающий может взять и доработать программу под себя, проверить безопасность или на базе Open source проекта сделать свое собственное приложение.
On-premise	Программные решения, которые устанавливаются на оборудование клиента.
MAST	Mobile Dynamic Application Security Testing (рус.: Тестирование мобильных приложений методом динамического анализа). Тестирование посредством использования класса инструментов для проведения динамического тестирования (тестирования на проникновения) и оценки безопасности мобильных приложений/сервисов, способных выявить уязвимости как на стадии тестирования, так и в ходе эксплуатации

СТИНГРЕЙ

Код	Тип требований	Вес	Описание требования	Важность	Платформа	Оценка (Стингрей)	Оценка (MobSF)	Оценка (RMS)	NowSecure*	AppKnox*	Quixxi*	ImmuniWeb*	Pradeo*	Ostorlab*	HCL AppScan Mobile*
ФТ-1	**Функциональные требования**	**10**	**Наличие on premise версии**	**Критичный**	**Общее**	4	4	4	2	2	0	0	0	0	0
АТ-1	**Архитектурные требования**	**10**	**Возможность запуска системы на опреационной сиситеме Astra Linux**	**Критичный**	**Общее**	4	3	3	0	0	0	0	0	0	0
ФТ-33	Функциональные требования	**10**	**Минимизация санкционного риска**	**Критичный**	**Общее**	4	4	4	0	0	0	0	0	0	0
ФТ-2	Функциональные требования	5	Возможность ручного взаимодействия с интерфейсом приложения при проведении сканирования мобильных приложений	Критичный	Android / iOS	**4**	**2**	**3**	**4**	**4**	**2**	**2**	**2**	**2**	**2**
ФТ-3	Функциональные требования	5	Возможность автоматического анализа Android и iOS приложения без необходимости ручного взаимодействия с приложением.	Критичный	Android / iOS	**4**	**0**	**0**	**3**	**0**	**0**	**0**	**0**	**3**	**0**
ФТ-4	Функциональные требования	4	Возможность записи последовательности действий для формирования автоматических тест-кейсов.	Высокий	Android / iOS	**4**	**0**	**0**	**3**	**0**	**0**	**0**	**0**	**0**	**0**
ФТ-5	Функциональные требования	4	Возможность формирования тест-кейсов без написания кода.	Высокий	Android / iOS	**4**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
ФТ-6	Функциональные требования	4	Возможность статического анализа декомпилированных/дизасемблированных приложений для операционных систем семейства Android и iOS.	Высокий	Android / iOS	**3**	**3**	**1**	**4**	**3**	**3**	**4**	**2**	**4**	**4**
ФТ-7	Функциональные требования	4	Возможность валидации записанного тест-кейса при изменении интерфейса приложения	Высокий	Android / iOS	**2**	**0**	**0**	**3**	**0**	**0**	**0**	**0**	**0**	**0**
ФТ-8	Функциональные требования	4	Возможность автоматического завершения сканирования при обнаружении незадекларированного поведения во время выполнения тестового сценария	Высокий	Android / iOS	**2**	**0**	**0**	**3**	**0**	**0**	**0**	**0**	**0**	**0**
ФТ-9	Функциональные требования	4	Возможность просмотра записи автоматического сканирования.	Высокий	Android / iOS	**4**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

СТИНГРЕЙ

Код	Тип требований	Вес	Описание требования	Важность	Платформа	Оценка (Стингрей)	Оценка (MobSF)	Оценка (RMS)	NowSecure*	AppKnox*	Quixxi*	ImmuniWeb*	Pradeo*	Ostorlab*	HCL AppScan Mobile*
ФТ-10	Функциональные требования	4	Возможность запуска Appium-скриптов для воспроизведения пользовательских сценариев для операционных систем семейства Android.	Высокий	Android	4	2	2	1	0	0	0	0	3	0
ФТ-11	Функциональные требования	3	Возможность определения обфускации Android приложения	Средний	Android	4	1	1	2	0	0	0	0	0	0
ФТ-12	Функциональные требования	3	Проведение анализа на проверку окружения (определение прав суперпользователя или работы на эмуляторе).	Средний	Android / iOS	2	0	0	4	0	0	0	0	0	0
ФТ-13	Функциональные требования	3	Возможность запуска поиска дефектов на ранее сформированном наборе результатов сканирования.	Средний	Android / iOS	4	1	1	1	1	1	1	1	1	1
ФТ-14	Функциональные требования	5	Возможность детальной настройки параметров сканирования (возможность детальной настройки\отключения любого модуля анализа, возможность изменения и добавления правил обнаружения уязвимостей)	Критичный	Android / iOS	4	1	1	4	0	0	0	0	1	0
ФТ-15	Функциональные требования	5	Идентификация типов уязвимостей, документированных в отраслевых источниках: OWASP Mobile Top 10 2017	Критичный	Android / iOS	4	2	1	4	1	2	2	1	2	2
ФТ-16	Функциональные требования	3	Возможность провести проверку на соответствие стандартам PCI DSS, OWASP MASVS, ОУД4, ГОСТ-57580	Средний	Общее	4	0	0	3	3	2	2	1	2	3
ФТ-17	Функциональные требования	3	Возможность добавления и проверки на соответствие собственным (внутренним) стандартам безопасности.	Средний	Общее	4	0	0	4	0	0	0	3	3	0
ФТ-18	Функциональные требования	2	Возможность работы с результатами сканирования до полного завершения процесса сканирования.	Низкий	Общее	4	1	0	2	2	2	2	2	4	2
ФТ-19	Функциональные требования	2	Возможность получения истории сканирований одного и того же приложения.	Низкий	Общее	4	2	0	4	4	3	3	4	4	4
ФТ-20	Функциональные требования	3	Возможность выгрузки коллекции сетевых запросов в формате HAR (HTTP Archive) для интеграции с системами динамического анализа backend-части системы	Средний	Общее	4	1	1	0	0	0	0	0	0	0

СТИНГРЕЙ

Код	Тип требований	Вес	Описание требования	Важность	Платформа	Оценка (Стингрей)	Оценка (MobSF)	Оценка (RMS)	NowSecure*	AppKnox*	Quixxi*	ImmuniWeb*	Pradeo*	Ostorlab*	HCL AppScan Mobile*
ФТ-21	Функциональные требования	3	Возможность загрузки приложений напрямую из магазинов приложений (RuStore, Google Play, Apple AppStore, Huawei AppGallery)	Средний	Общее	4	0	0	4	0	0	0	0	4	4
ФТ-22	Функциональные требования	3	Возможность настройки мониторинга появления новых версий приложений в магазинах приложений, их автоматическая загрузка и запуск сканирования	Средний	Общее	4	1	1	4	3	3	3	3	3	3
ФТ-23	Функциональные требования	5	Наличие рекомендаций по исправлению уязвимостей на русском языке, наличие ссылок на индустриальные стандарты	Критичный	Общее	4	1	0	2	2	2	2	2	2	2
ФТ-24	Функциональные требования	3	Возможность просмотра и загрузки информации, собранной во время работы приложения	Средний	Общее	4	3	3	2	3	1	2	4	4	4
ФТ-25	Функциональные требования	3	Наличие ролевой/Проектной модели доступа к уязвимостям с возможностью модификации / адаптации модели	Средний	Общее	4	0	0	2	2	2	4	4	4	4
ФТ-26	Функциональные требования	5	Возможность интеграции с корпоративными сервисами LDAP/Active Directory	Критичный	Общее	4	0	0	0	0	0	0	0	0	0
ФТ-27	Функциональные требования	3	Возможность интеграции с дефект-трекерами (Jira/Yandex Tracker и т.д.)	Средний	Общее	1	1	0	4	0	0	0	0	2	2
ФТ-28	Функциональные требования	5	Возможность интеграции с системами непрерывной интеграции (CI) TeamCity/Jenkins/Gitlab CI или наличие CLI для работы с инструментом	Критичный	Общее	3	2	0	4	2	2	3	3	3	3
ФТ-29	Функциональные требования	5	Возможность использования полного функционала системы с использованием REST API и возможность написания кастомизированной интеграции для инструмента, используя предоставленный API	Критичный	Общее	4	3	1	4	4	4	4	4	4	4
ФТ-30	Функциональные требования	3	Возможность генерации отчётов в PDF-формате	Средний	Общее	4	4	0	4	4	4	4	4	4	4
ФТ-31	Функциональные требования	5	Наличие регулярных обновлений базы уязвимостей, правил обнаружения уязвимостей.	Критичный	Общее	4	1	1	4	4	4	4	4	4	4

СТИНГРЕЙ

Код	Тип требований	Вес	Описание требования	Важность	Платформа	Оценка (Стингрей)	Оценка (MobSF)	Оценка (RMS)	NowSecure*	AppKnox*	Quixxi*	ImmuniWeb*	Pradeo*	Ostorlab*	HCL AppScan Mobile*
ФТ-32	Функциональные требования	2	Наличие поддержки русского языка	Низкий	Общее	4	0	0	0	0	0	0	0	0	0
АТ-2	Архитектурные требования	5	Возможность полноценно функционировать в закрытом контуре без необходимости использования внешних сервисов (в т. ч. и вендора).	Критичный	Общее	4	4	4	2	2	0	0	0	0	0
АТ-3	Архитектурные требования	4	Наличие встроенного механизма мониторинга состояния компонент и АПИ съема метрик (healthcheck).	Высокий	Общее	3	1	1	0	0	0	0	0	0	0
АТ-4	Архитектурные требования	4	Возможность настройки парольной политики для локальной аутентификации	Высокий	Общее	4	0	0	0	0	0	0	0	0	0
АТ-5	Архитектурные требования	4	Возможность горизонтального масштабирования системы	Высокий	Общее	1	1	1	0	0	0	0	0	0	0
			Решения, отмеченные желтым, не работают на территории РФ		Формат решения	Есть On-Premise и SaaS	Open Source	Open Source	Частично	Частично	Нет	Нет	Нет	Нет	Нет

AppKnox - On Premise поставляется в виде аппаратно-программного комплекса от 10 приложений, но тестирование решения возможно провести только в облачном формат
NowSecure - есть On premise версия в виде отдельного ноутбука с двумя телефонами.

Итого	**36**	**15**	**5**	**26**	**21**	**19**	**23**	**25**	**27**	**27**
С учетом коэффициентов	**592**	**264**	**210**	**349**	**191**	**145**	**163**	**164**	**234**	**192**
Максимум	**825**	**825**	**825**	**825**	**825**	**825**	**825**	**825**	**825**	**825**
% от максимального значения	72%	32%	25%	42%	23%	18%	20%	20%	28%	23%