**УДК 004** **Информационные технологии**

***Пантелеев Николай Николаевич,*** *преподаватель военного учебного центра, «Цикл связи» РТУ МИРЭА, РФ, г. Москва*

***Панов Сергей Сергеевич,*** *студент военного учебного центра Российского Технологического Университета МИРЭА, РФ, г. Москва*

***Кудояр Владислав Романович,*** *студент военного учебного центра Российского Технологического Университета МИРЭА, РФ, г. Москва*

# АНАЛИЗ И ВЫБОР СТРУКТУРЫ ОЦЕНКИ РИСКОВ ДЛЯ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ

**Аннотация:** Для конечных пользователей доступно множество корпоративных приложений для использования в различных областях, включая логистику, финансы и производство. С появлением облачных вычислений организациям крайне важно определить риски, связанные с принятием облачных решений или приложений, чтобы обеспечить конфиденциальность информации. Проблема заключается в оценке рисков приложений в контексте информационной безопасности. Очень важно адаптировать правильную стратегию оценки для упреждающего реагирования на ситуацию в этой области. Мы проанализировали различные структуры оценки рисков, которые помогут оценить приложения в корпоративных информационных системах, взяв за основу CWRAF (Common Weakness Risk Analysis Framework) и CVSS (Common Vulnerability Scoring System), как два доминирующих подхода в процессе оценки рисков корпоративных приложений.

**Ключевые слова:** облачные вычисления; риск; подход к оценке риска; пользователи облачных вычислений.

**Annotation:** A lot of enterprise applications are available for the end users to use in different domains including logistics, finance and manufacturing. In the advent

of cloud computing, it is imperative for organizations to determine risks involved in adopting cloud-based solutions or applications to ensure confidentiality of information. The problem is the risk assessment of enterprise applications from the context of information security. It is very essential to adapt the right risk assessment strategy to handle the security situation proactively. We analyze the different risk assessment frameworks which would help to evaluate applications in enterprise information systems. We have evaluated both CWRAF (Common Weakness Risk Analysis Framework) и CVSS (Common Vulnerability Scoring System) as two predominant frameworks in the risk assessment process.

**Keywords:** cloud computing, risk, risk assessment approach; cloud computing consumers.

На риски всегда нужно смотреть с негативной точки зрения. Оценка и идентификация рисков — это благоприятный момент для определения возможности повышения безопасности и устранения лазеек в системе безопасности. Согласно ISO 31000:2018 риск (risk) определяется как «влияние неопределенности на цели» [10]. Оно может быть положительным и/или отрицательным, и может способствовать реализации контрмер и устранению угроз, создавать или приводить к возникновению возможностей и угроз.

Поскольку внедрение облачных вычислений растет день ото дня, поскольку оно обладает преимуществами масштабируемости, производительности и гибкости, это также означает, что пользователям облачных решений необходимо убедиться в том, что они совершают правильные действия, когда внедряют их в существующие бизнесс-процессы. Для пользователей корпоративных информационных систем крайне важно обеспечить минимальную поверхность рисков при таком внедрении или минимизировать риски при принятии таких инициатив [1].

Согласно крупному опросу о внедрении облачных технологий в четвертом квартале 2014 года, проведенному компанией GigaOMResearch на базе NorthBridge с участием 1358 респондентов, 49% уже внедрили облачные

технологии для увеличения доходов и разработки новых продуктов, а 45% задумываются о том, чтобы внедрить облачные технологии в организации. Это показывает уровень значимости растущего спроса на внедрение облачных вычислений. Принятие приложений SaaS увеличилось с 13% в 2011 году до 72% в 2014 году [2]. Готовность к внедрению облачных вычислений зависит от а) выгоды, которую организация собирается получить, б) технической осуществимости переноса устаревшего или существующего приложения в облако и, наконец, в) рисков, связанных с переходом на облачные приложения.

Хотя внедрение облака помогает быстро повысить уровень обслуживания и производительность, оно также может повысить контроль над рисками. Поскольку такие платформы, как Azure и Amazon, сделали облачное администрирование фундаментально простым с оплатой по мере использования, качественно плохое управление данными на этих порталах без понимания последствий может привести к финансовым рискам, если оно не будет надлежащим образом обработано. Когда организации разбросаны по разным географическим точкам, доступность услуг через разные центры обработки данных в распределенной среде должна учитываться.

Безопасность облачных приложений не заканчивается тем, что разработчики заботятся обо всех угрозах на этапе разработки, включая различные факторы, такие как платформа развертывания, права доступа, уязвимости в физической среде развертывания и т. д., поэтому очень важно устранять риски безопасности с точки зрения бизнесс-пользователя, основанные на его потребностях в безопасности. Бизнесс-пользователь должен осознавать влияние возможного нарушения безопасности, чтобы можно было снизить такие риски.

В этом документе предпринята попытка определить структуры рисков для оценки облачных приложений SaaS (Software as a service) в контексте пользователей коммерческих информационных систем и помочь им выбрать правильные структуры рисков.

***Необходимость в системах оценки рисков.*** Хотя существуют различные методологии анализа рисков, не существует конкретной основы, которую можно было бы всесторонне применить или принять. Исследователи [3] приходят к выводу, что отсутствует структурированный метод, который можно было бы использовать для оценки рисков, чтобы потребители облачных вычислений могли использовать свои ресурсы, дабы безопасно ускорить внедрение облачных технологий и использовать преимущества текущих тенденций в технологиях через облачные вычисления.

***Объем оценки риска.*** Существует ряд известных опасений по поводу облачных вычислений, которые необходимы для коммерческих организаций, изложенных в Business News Daily [13]

- Кибератаки
- Внутренние угрозы
- Ответственность, установленная законом
- Отсутствие стандартизации
- Отсутствие поддержки
- Другие риски

***Существующая оценка рисков.*** Различные категории облачных вычислений, такие как IaaS (Infrastructure as a service), PaaS (Platform as a service) и SaaS (Software as a service), должны быть сосредоточены на оценивании при проведении анализа рисков в период внедрения облачных технологий. Факторы, которые могут повлиять на внедрение облачных технологий, являются технологические, организационные и экономические.

***Существующие облачные платформы.*** Большинство виртуализированных инфраструктур развернуты на облачных платформах IaaS (инфраструктура как услуга). Они подразделяются на две широкие категории, как указано ниже:

*Платформы IaaS (Проприетарные):*

- Microsoft Azure.
- Amazon.

*Платформы IaaS (Открытые):*

- OpenStack.
- Apache CloudStack.

Существует возможность даже развернуть виртуальные ресурсы или клиентские инструменты для управления виртуальными машинами, чтобы проверить их поведение.

Критические факторы должны быть оценены в стандартной облачной конфигурации и проанализированы существующие доступные методологии оценки рисков облачных вычислений, а также найдена методология, которая позволит конечному пользователю легко анализировать и внедрять структуру. В этом документе будет предпринята попытка определить существующие структуры оценки рисков, доступные для облачных вычислений, и будут оценены их плюсы и минусы путем внедрения некоторых факторов риска в облачные приложения путем моделирования или развертывания их в облаке (таблица 1).

Таблица 1 – Пять важных характеристик облачной среды [14].

| Номер | Характеристика | Влияние |
|---|---|---|
| 1 | По требованию, самообслуживание | Предоставление услуг по запросу (хранилище, вычисления и т. д.) |
| 2 | Объединение ресурсов | Совместное использование ресурсов, таких как память, пропускная способность и т. д. |
| 3 | Измеренное обслуживание | Измерение использования, оплата по мере использования |
| 4 | Быстрая гибкость | Масштабирование |
| 5 | Широкий доступ к сети | Ресурсы и приложения, доступные по сети |

***CWRAF.*** Common Weakness Risk Analysis Framework помогает организациям, заинтересованным в обнаружении слабых сторон, выбрать решение, которое они выделили на основе CWE (Common Weakness Enumeration). Ключевым аспектом этой структуры является сосредоточение внимания на слабых местах, существующих в целевой системе. CWE используется популярными бюллетенями по безопасности, такими как OWASP (Open Web Application Security Project). CWRAF также использует CWSS (Common Weakness Scoring System), который представляет собой механизм, используемый для оценки серьезности CWE, выявленной в корпоративных приложениях. Он помогает количественно определить слабые стороны и действует как общая структура для разработчиков [16].

CWRAF исходит из того, что, хотя программное обеспечение является одним и тем же, приложение и его использование будут варьироваться от пользователя к пользователю в зависимости от их потребностей в безопасности, и оценка рисков также будет соответственно различаться. Инициатива CVE сопоставила и задокументировала более 47 000 общеизвестных уязвимостей в коммерческом программном обеспечении и программном обеспечении с открытым исходным кодом, используемом по всему миру (Рисунок 1) [4].

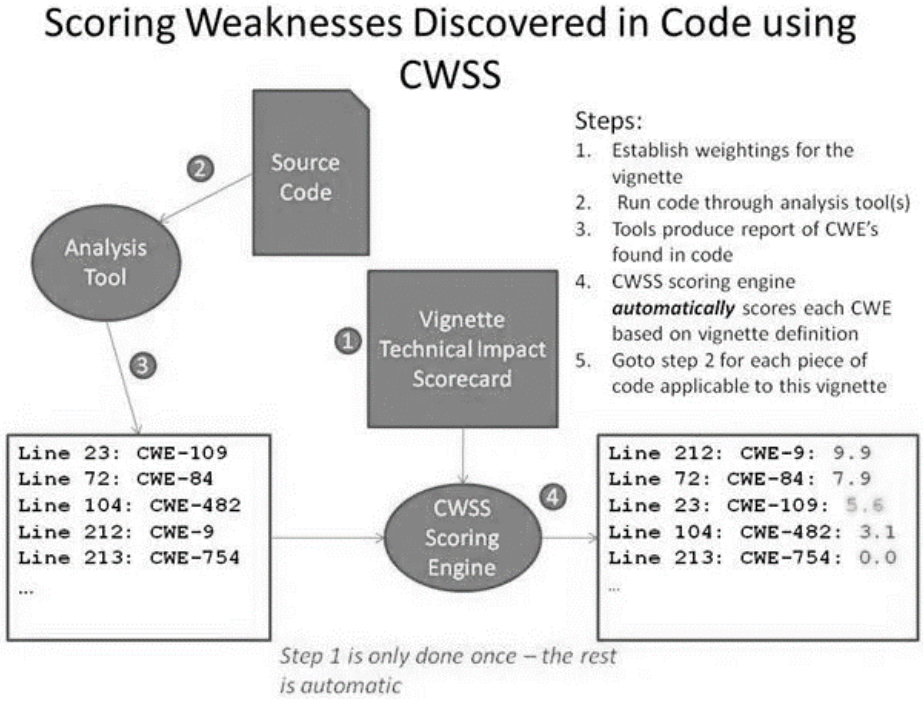


Рисунок 1. Источник CWRAF – оценка уязвимостей

Чтобы найти Base Finding Subscore, Attack Surface Subscore and Environmental Subscore необходимо:

1. Base = [ (10 * TechnicalImpact + 5*(AcquiredPrivilege + AcquiredPrivilegeLayer) + 5*FindingConfidence) * f (TechnicalImpact) * InternalControlEffectiveness ] * 4.0

2. f (TechnicalImpact) = 0 if TechnicalImpact = 0; otherwise f (TechnicalImpact) = 1.

3. AttackSurfaceSubscore = [ 20*(RequiredPrivilege + RequiredPrivilegeLayer + AccessVector) + 20*DeploymentScope + 15*LevelOfInteraction + 5*AuthenticationStrength ] / 100.0

4. EnvironmentalSubscore = [ (10*BusinessImpact + 3*LikelihoodOfDiscovery + 4*LikelihoodOfExploit) + 3*Prevalence) * f(BusinessImpact) * ExternalControlEffectiveness ] / 20.0.

В основном оценка CWE выполняется на основе следующих показателей:

- Base Finding Subscore: отражает неотъемлемый риск слабости, уверенность в точности результатов и силу средств контроля.
- Attack Surface Subscore: барьеры, которые атакующий должен преодолеть, чтобы воспользоваться уязвимостью.
- Environmental Subscore: характеристики уязвимости, специфичные для конкретной среды или рабочего контекста.

***CVSS.*** Общая система оценки уязвимостей (CVSS) представляет собой открытую структуру для передачи информации о характеристиках и серьезности уязвимостей программного обеспечения [17]. FIRST — это некоммерческая организация, базирующаяся в США. CVSS имеет структуру риска версии 3.0, которая управляет оценкой уязвимостей на основе базовой и временной группы.

Ниже приведены аспекты, над которыми будет работать оценка рисков CVSS:

- Базовая оценка (Base score) представляет наиболее фундаментальные, неизменные качества уязвимости.

- Временные метрики (Temporal Metrics), которые представляют зависящие от времени качества уязвимости.
- Метрики окружающей среды (Environmental Metrics), которые представляют характерные для реализации и среды качества уязвимости.

Для поиска Base Finding Subscore и Environmental Subscore необходимо:

1. Base Score = round_to_1_decimal (((0.6*Impact) + (0.4*Exploitability)–1.5)*f(Impact)) Temporal Score = round_to_1_decimal (BaseScore*Exploitability*RemediationLevel*ReportConfiden ce)
2. EnvironmentalScore = round_to_1_decimal ((AdjustedTemporal +(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistrib ution)

***Система принятия решений об облачных рисках (CRDA).*** Платформа оценки облачных рисков основана на стандарте ISO 31000. Руководящие принципы CRDA основаны на стандарте ISO 31000. CRDA фокусируется на компоненте «Процесс» стандарта для системы принятия решений об облачных рисках, как показано на рисунке 2.


Рисунок 2. Система принятия решений об облачных рисках (CRDA).

Анализ проводится на основе областей контроля риска, вероятности риска и воздействия риска. В процессе идентификации риски классифицируются по следующим группам рисков, таким как комплаенс-риски, стратегические риски, операционные риски, рыночные и финансовые риски. Риски измеряются в диапазоне от 0 до 25 с такими рейтингами, как очень высокий, высокий, умеренный, низкий и очень низкий. На основе формулы риска функции вероятности x воздействия с возможной оценкой от 1 до 25.

***Методология исследования.*** Наш подход основан на использовании существующих структур и выявлении проблем для реализации, а также рекомендует шаги для устранения этих проблем. Ниже приведены этапы процесса:

1. Определить существующую структуру, которая подходит для облачной среды или облачных решений при выявлении рисков безопасности.

2. Определить инструменты, которые помогут выявить уязвимости или недостатки безопасности, существующие в 3 выбранных приложениях.

3. Сопоставить слабые места и уязвимости по отношению к выбранных структурам.

4. Применить методологию расчета рисков с использованием структуры

5. Сравнить и обрисовать результаты на основе того, как оцениваются рейтинги оценки риска.

Кроме того, 10 принципов безопасности, определенных Ассоциацией аудита и контроля информационных систем (ISACA) для сред оценки рисков, предлагают руководство по выбору правильной структуры оценки рисков для облачного приложения [5].

Важно, чтобы используемая структура соответствовала существующим аспектам безопасности отрасли. Для платформы очень важно постоянно обновляться и идти в ногу с меняющимся технологическим ландшафтом. Основанная на стандартах структура не устраняет напрямую угрозы и уязвимости, а существующая в облачных приложениях обеспечивает структуру управления, основанную на отраслевых стандартах.

В этом контексте выбраны две платформы: CWRAF и CVSS, потому что они имеют стандартизированные и систематизированные слабые места/угрозы, которые обновляются, в отличие от таких стандартов, как COBIT или ISO, которые зависят от общих методов выявления слабых мест/уязвимостей. Более того, такие структуры, как COBIT и фреймворк принятия решений об облачных рисках CRDA, нельзя использовать независимо.

***Случаи применения.*** Приложение SaaS (Software as a service) рассматривается как наша область оценки рисков, поскольку приложения SaaS (Software as a service) могут пересекаться с облачной платформой, имеющей дело с приложениями, данными, средой выполнения, промежуточным ПО,

операционной системой, виртуализацией, серверами, хранилищем и сетью.

Для оценки выбранной платформы используются система управления контентом (CMS), управление взаимоотношениями с клиентами (CRM) и инструмент финансового управления. Причина их выбора заключается в том, что большинству пользователей требуются такие приложения для эффективного выполнения своих операций. Эти приложения представляют собой облачные приложения, которые также могут быть размещены на локальном сервере за брандмауэром. Приложения типа SaaS в рамках этих вариантов использования (таблица 2).

Таблица 2 – Рассматриваемые приложения

| S.no | Application | Rationale |
|---|---|---|
| 1 | Zurmo CRM | CRM (Управление взаимоотношениями с клиентами), используется бизнесом для управления отношениями с клиентами |
| 2 | Wordpress | Широко используемая CMS (система управления контентом) |
| 3 | Webzash | Финансовое программное обеспечение |

***Wordpress*** — это ведущая система управления контентом с открытым исходным кодом, используемая для разработки веб-сайтов для деловых целей или управления корпоративными блогами. Эта система управления контентом основана на PHP.

***Zurmo CRM*** — это инструмент управления взаимоотношениями с клиентами, который позволяет управлять продажами с помощью значков и баллов. Этот инструмент помогает отслеживать возможности, интересы и контакты и помогает эффективно управлять конвейером продаж.

***WebZash*** — это система учета с двойной записью на основе PHP с открытым исходным кодом. Он имеет такие возможности, как план счетов, управление счетами, выполнение финансовых транзакций, квитанции и платежи. Он имеет дополнительные функции, такие как отчеты, аутентификация, роли, прибыль и убытки и баланс.

***Используемые инструменты***

1. OpenVAS - Фреймворк, состоящий из нескольких сервисов и утилит, позволяющий производить сканирование узлов сети на наличие уязвимостей и управление уязвимостями

2. Vega - сканер веб-уязвимостей, созданный канадской компанией Subgraph и распространяемый как инструмент с открытым исходным кодом

3. RIPS – инструмент статического анализа кода

***Реализация.*** По мере того, как многоуровневое облачное приложение проходит через IaaS (инфраструктура как сервис), PaaS (платформа как сервис) и SaaS (Приложение как сервис), важно искать способы обнаружения рисков путем проведения соответствующего анализа уязвимостей с использованием правильных инструментов. Затем на основе результатов этих инструментов необходимо провести количественную оценку рисков для соответствующей приоритизации рисков и усилий, необходимых для их снижения.

На рисунке 3 представлен подход, выбранный для определения оценки риска для уязвимостей, выявленных с помощью CWRAF и CVSS, в соответствии с их соответствующими рекомендациями. Во-первых, приложение было развернуто локально для статического анализа кода. Статический анализ кода был выполнен с использованием инструмента с открытым исходным кодом под названием RIPS. В данном случае используется RIPS, поскольку все 3 приложения используют PHP в качестве кодовой базы (рисунок 4).

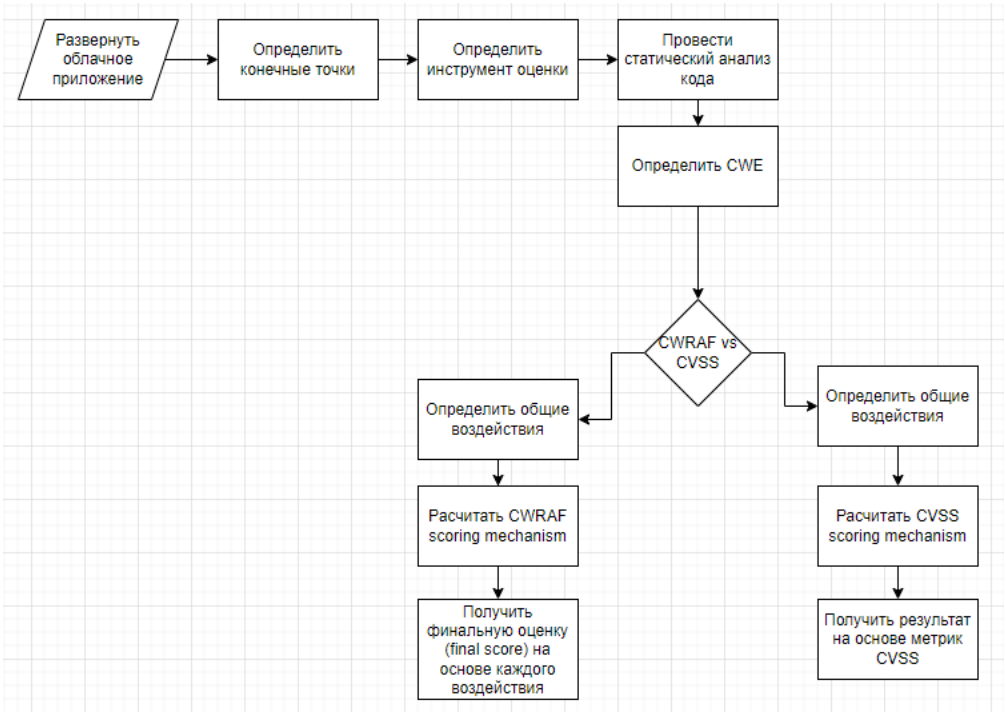


Рисунок 3 - Подход определения оценки риска для уязвимостей, выявленных с помощью CWRAF и CVSS.

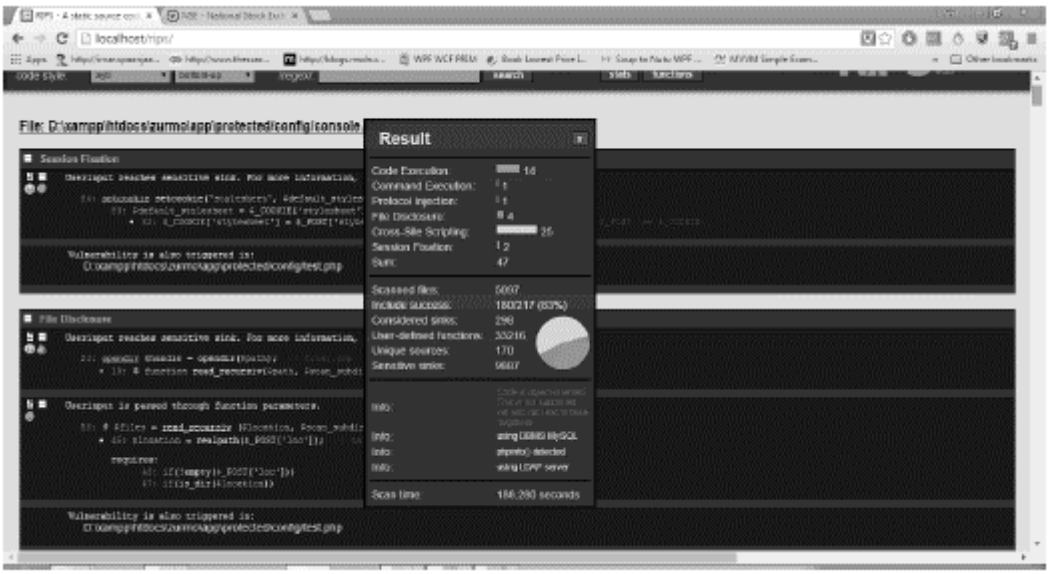


Рисунок 4 - Анализ кодовой базы Zurmo CRM с использованием RIPS.

Следующим шагом все три приложения были развернуты в облаке на основе определенной конечной точки. Затем конечная точка передается в качестве входных данных для приложений OpenVAS и Vega для выявления уязвимостей или анализа. Vega используется для анализа с конечной точкой

приложения в качестве входных данных и настраивается для анализа. Это инструмент на основе Java, который может быть полезен при поиске XSS (межсайтовых скриптов), SQL-инъекций и других уязвимостей (рисунок 5).

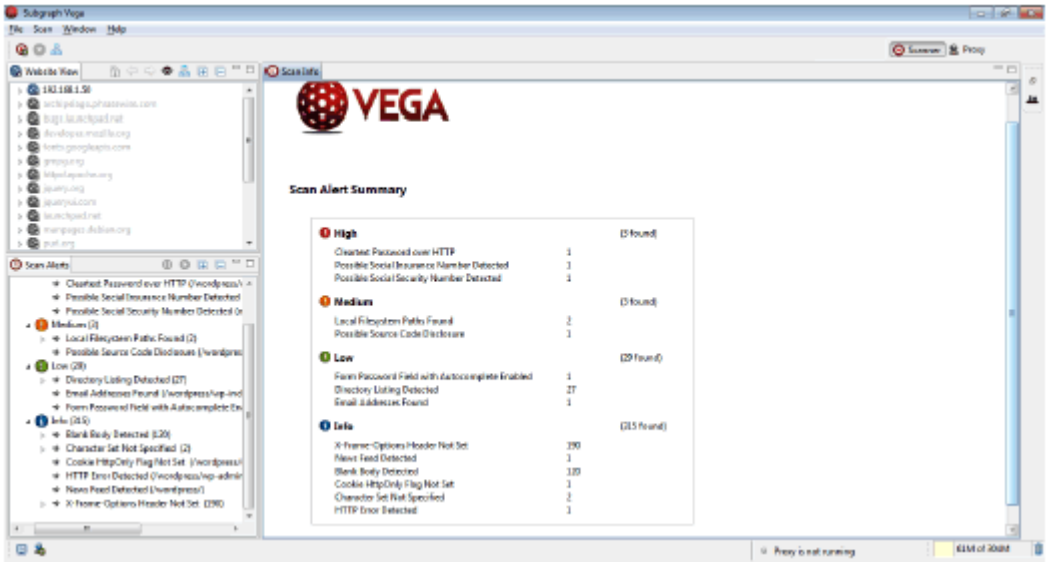


Рисунок 5 – Анализ слабых мест приложения через Vega

CWRAF в основном приближается к оценке с 8 техническими воздействиями. При попытке найти связанные с этим риски, приложениям, находящимся в сфере охвата, присваивается приоритет с помощью CWRAF. Оценка недостатков, выявленных в облачных приложениях, будет определяться CWSS в сочетании с подходом, определенным в CWRAF. Ключевым преимуществом использования CWRAF является получение списка рисков относительно бизнес-контекста. После того, как расчеты CWRAF выполнены, для принятия необходимых мер необходим список Top N, характерный для бизнес-приложения.

С другой стороны, CVSS вычисляет базовую оценку, временную оценку и оценку среды, чтобы дать общее представление о риске, связанном с конкретной уязвимостью. Хотя базовая оценка указывает на критические уязвимости, оценка окружающей среды указывает на значимость проблемы в зависимости от контекста. Базовая оценка сильно зависит от факторов воздействия и возможности эксплуатации.

***Заключение.*** Анализ кода или анализ уязвимостей выполняется с помощью таких инструментов, как Vega и RIPS. В результате сканирования исходного кода приложений выявляются проблемы. Некоторые примеры таких проблем, часто встречающихся в приложениях, приведены ниже для справки. Из Таблицы 3 следует, что проблемы, связанные с CWE-ID, могут привести к серьезным бизнес-рискам, если их оставить без внимания.

Таблица 3 – определение CWE на основе проблем, выявленных во время статического анализа кода в 3 приложениях.

| **CWE ID** | **Common Consequences** |
|---|---|
| CWE-384: Фиксация сеанса | Контроль доступа<br>Получение привилегии |
| CWE-113: Неправильная нейтрализация последовательностей CRLF в Заголовки HTTP («Разделение ответа HTTP») | Целостность<br>Контроль доступа<br>Изменение данных приложения<br>Получение привилегий |
| CWE-691: Недостаточный контроль потоком управления | Другие<br>Изменение логики выполнения |
| CWE-79: Неправильная нейтрализация ввода во время создания веб-страницы («Межсайтовый скриптинг») | Контроль доступа<br>Конфиденциальность<br>Обход механизма защиты<br>Чтение данных приложения<br>Целостность<br>Доступность<br>Выполнение неавторизованного кода или команды |

Чтобы понять влияние этих CWE, для этих приложений были рассчитаны оценки риска для CWRAF и факторов окружающей среды для CVSS. Например, оценки на основе CVSS рассчитываются на основе базовой оценки, которая в первую очередь зависит от воздействия и возможности использования. Согласно расчетам CVSS, CWE-73, CWE-538 и CWE-359 имеют более высокий базовый балл, который требует внимания (Рисунок 6).

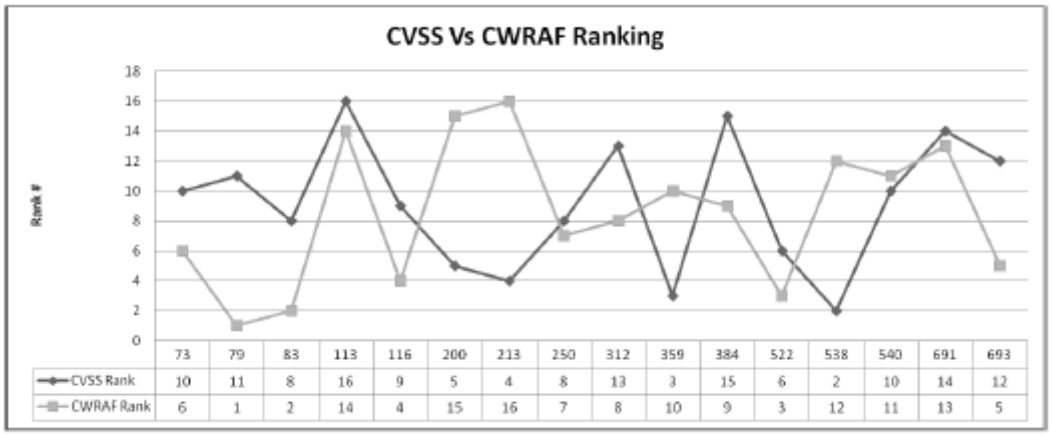


Рисунок 6 - CWRAF против CVSS

Что касается расчета CWRAF, CWE-79, CWE-83 и CWE-522, по-видимому, имеют более высокий приоритет для исправления. Это основано исключительно на оценке расчетов аналитика безопасности по контексту, определяемому бизнес-потребностями, и расчету CWRAF.

Ниже приведены некоторые из проблем, которые необходимы для улучшения оценки рисков облачной безопасности и для эффективного управления жизненным циклом рисков:

1. Оценка рисков должна быть непрерывным процессом, который должен осуществляться с помощью эталонной архитектуры, согласованной с существующей облачной и ИТ-экосистемой.

2. Риск возникает во всем облаке из-за подключенной сети, поэтому обмен информацией с хорошим подключением должен быть обеспечен с помощью существующих протоколов или новых средств.

3. В контексте общедоступного облака могут возникать угрозы и уязвимости, которые могут предшествовать корпоративным приложениям.

4. Среды оценки рисков должны быть постоянно бесшовно интегрированы с базами данных CWE, CVE, ExploitDB и другими подобными базами данных для создания целостных возможностей.

Существующие платформы, такие как CWRAF и CVSS, в целом не являются всеобъемлющими для обработки интегрированного жизненного цикла.

Потребность в комплексном подходе к управлению рисками больше всего нужна во всей экосистеме для эффективного управления рисками на облачных платформах.

Возможный подход к автоматизации проверки уязвимостей при непрерывной интеграции или новом развертывании может быть оценен на будущее. Внедрение структуры оценки рисков должно быть интегрировано с рабочим процессом и инструментом визуализации данных для повышения эффективности. Существует возможность усовершенствования архитектуры для реализации таких аспектов интеграции, как типы файлов, сценарии распределенной вычислительной среды.

**Библиографический список:**


1. Стоун Г. Cloud Risk Decision Framework. Microsoft – 2014.
2. Скок МЮ. Исследование «Будущее облачных вычислений» – 2014.
3. Дрисси С. Survey: Risk assessment for cloud computing. Int J Adv Comput Sci Appl. – 2013. – №4. – С. 143-147.
4. Мартин Р. The Software Industry's "Clean Water Act" Alternative. IEEE – 2013.
5. Воградский Д. Cloud Risk-10 Principles and a Framework. ИСАКА J 2012; 5: 1-11.
6. [Электронный ресурс] http://www.iso.org/iso/home/standards/iso 31000.htm – управление рисками – руководящие принципы (дата обращения: 05.02.2022).
7. [Электронный ресурс] http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html – Облачные вычисления: Руководство для малого бизнеса (дата обращения: 05.02.2022).
8. [Электронный ресурс] https://cloudsecurityalliance.org/csaguide.pdf – Руководство по безопасности для важнейших областей применения облачных вычислений (дата обращения: 05.02.2022).
9. [Электронный ресурс] http://cwe.mitre.org/index.html –

Разработанный сообществом список типов слабых мест программного и аппаратного обеспечения (дата обращения: 05.02.2022).

10. [Электронный ресурс] https://www.first.org/cvss – Общая система оценки уязвимостей (дата обращения: 05.02.2022).