

Севастопольский государственный университет
Кафедра информационных технологий и компьютерных систем

Выпускная квалификационная работа магистра на тему:

Исследование процессов обеспечения безопасности облачных сред

Магистрант:
ст.гр. ИВТ/м-31-з, Умеров А.Р.

Научный руководитель:
к.т.н., доцент, Мащенко Е.Н.

2017 г.

Цели и задачи исследования

Цель: повышение эффективности процессов обеспечения информационной безопасности облачных сред

Задачи:

- обзор составных частей облачной инфраструктуры
- анализ технологий используемых облачными поставщиками
- исследование специфики применений облачных вычислений в России
- исследование проблем безопасности облачных вычислений
- исследование уязвимостей в облачной среде

Входные и выходные данные

Входные данные:

- структура и характеристики облачной среды
- перечень угроз и уязвимостей
- перечень характеристик качества системы ИБ
- облачная инфраструктура

Выходные данные:

- структура системы информационной безопасности
- ПО для получения данных об уязвимостях
- анализ ПО используемого в облачных вычислениях
- информация о проблемах безопасности в облачной среде

Составные части и технологии облачной инфраструктуры

Составные части:

- клиентские устройства
- сетевая среда доступа
- специализированное ПО
- центр обработки данных

Технологии:

- виртуализация
- оркестратор
- список (каталог) услуг
- портал самообслуживания
- система тарификации и выставления счетов (биллинг)

Проблемы стандартизации облачных вычислений

Проблемы:

- не существует единого стандарта безопасности
- множество корпоративных стандартов
- репутация компании играет важную роль



OASIS



NIST

**National Institute of
Standards and Technology**
U.S. Department of Commerce

CSA *cloud
security
alliance®*



Стратегически важные области безопасности

Security Guidance for Critical Areas of Focus in Cloud Computing

- архитектурные решения сред облачных вычислений
- государственное и корпоративное управление рисками
- легальное и электронное открытие
- соответствие техническим условиям и отчетность
- управление жизненным циклом информации
- портативность и совместимость
- традиционная безопасность, восстановление
- работа центра обработки данных
- реакция на риски, уведомление и обучение
- прикладная безопасность
- криптография и управление ключами
- идентификация и управление доступом
- виртуализация

Специфика российского рынка облачных услуг

- наблюдается большой рост
- отсутствует явный монополист
- рынок облачных услуг разнообразен
- качество услуг растет
- влияние ФЗ №242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»

Крупнейшие поставщики услуг ЦОД в России

| # | Название компании | Количество доступных стойко-мест | Количество размещенных стойко-мест | Загруженность мощностей (%) |
|---|-------------------|----------------------------------|------------------------------------|-----------------------------|
| 1 | Ростелеком | 3 900 | 3 432 | 88 |
| 2 | DataLine | 3 703 | 2 988 | 81 |
| 3 | DataPro | 3 000 | нет данных | нет данных |
| 4 | Linxtelecom | 2 040 | нет данных | нет данных |
| 5 | Selectel | 1 500 | 1 200 | 80 |
| 6 | Stack Group | 1 400 | 854 | 61 |
| 7 | Ай-Теко | 1 200 | 960 | 80 |

Проблемы безопасности в облачной среде

- утечка данных
- компрометация учетных записей и обход аутентификации
- взлом интерфейсов и API
- уязвимость используемых систем
- кража учетных записей
- инсайдеры-злоумышленники
- целевые кибератаки
- перманентная потеря данных
- недостаточная осведомленность
- злоупотребление облачными сервисами
- DDoS-атаки
- совместные технологии, общие риски

Результаты системного анализа

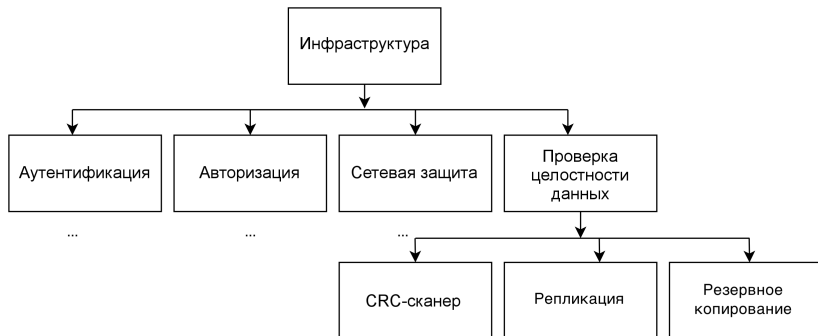
Функции:

- авторизация и аутентификация пользователей
- сетевая защита
- идентификация и обработка инцидентов
- предоставление доступа к услугам
- мониторинг

Подсистемы:

- подсистема аутентификации
- подсистема авторизации
- подсистема сетевой защиты
- подсистема проверки целостности данных

Принцип иерархий



Результаты вариантного анализа

Цель: выбор гипервизора

Метод анализа иерархий:

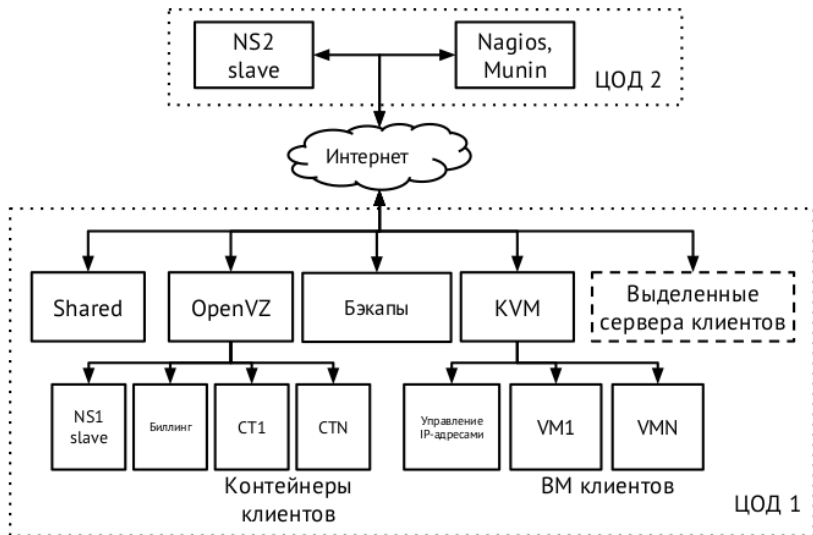
- альтернативы: KVM, Hyper-V, VMware vSphere
- критерии: цена, масштабируемость, отказоустойчивость, интерфейсы управления
- предпочтение отдано альтернативе B (VMware vSphere)



Microsoft
Hyper-V



Структурная схема облачной среды



Архитектура информационной безопасности

Ограниченный физический и логический доступ к периметру оборудования в ЦОД

Управление
доступами
администратора

Управление
изменениями

Управление
журналами

Защита памяти

Управление
конфигурациями и
уязвимостями

Сегментация сети
и контроль
трафика

Мониторинг и
управление
целостностью

Управление
приложениями

Шифрование
данных

Расширенное
обнаружение и
реакция

Экранирование
уязвимостей

Антивирус

Программно-специфическая защита: WAF, DAM, DoS

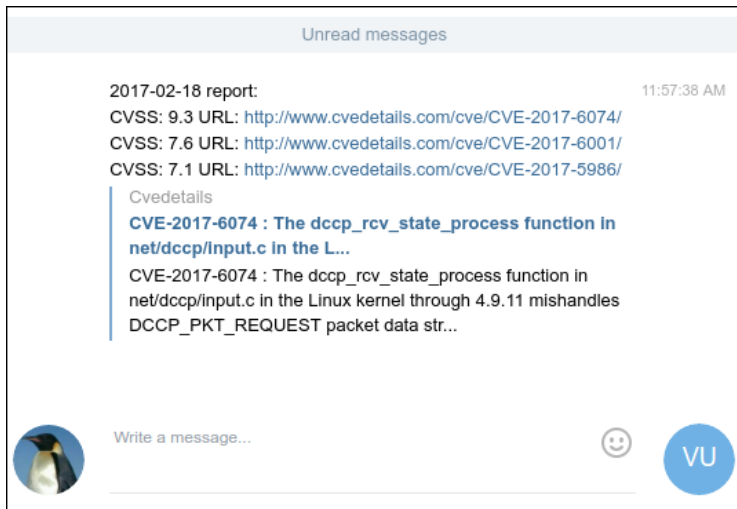
Экспериментальные исследования

Наиболее опасные критические уязвимости 2016 г.

| CVE ID | CVSS | Тип уязвимости | ПО |
|---------------|-------------|---|--------------|
| CVE-2016-5195 | 7.2 | Получение привилегий | Linux Kernel |
| CVE-2016-6258 | 7.2 | Получение привилегий | Xen |
| CVE-2016-5696 | 5.8 | Получение данных | Linux Kernel |
| CVE-2016-3710 | 7.2 | Запуск кода | QEMU |
| CVE-2016-8655 | 7.2 | Получение привилегий, DoS | Linux Kernel |
| CVE-2016-4997 | 7.2 | Получение привилегий, доступ к памяти, DoS | Linux Kernel |
| CVE-2016-4484 | 7.2 | Получение привилегий | CryptSetup |
| CVE-2016-6309 | 10.0 | DoS, запуск кода | OpenSSL |

Экспериментальные исследования

Уведомление скрипта мониторинга в Telegram



Результаты

- обзор литературных источников и открытых стандартов
- анализ рынка облачных услуг
- определение угроз безопасности облачных вычислений и методов их решения
- системный анализ безопасности облачной среды
- вариантный анализ для выбора оптимальной альтернативы
- сбор данных по наиболее опасным уязвимостям в ПО
- практическая эксплуатация уязвимости CVE-2016-5195
- разработка системы сбора данных по уязвимостям

Выводы

- проанализированы существующие проблемы и стандарты безопасности облачных вычислений
- предложены способы решения данных проблем
- рассмотрена специфика предоставления облачных услуг зарубежных и отечественных поставщиков
- проанализированы опасные уязвимости за 2016 г.
- описаны входные и выходные данные, функции системы безопасности, произведена декомпозиция системы и описана связь между ее элементами
- произведен сравнительный анализ гипервизоров
- эксплуатирована уязвимость CVE-2016-5195
- разработана система мониторинга уязвимостей