Министерство науки и высшего образования Российской Федерации федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Факультет инфокоммуникационных технологий

**Основы кибербезопасности**

Практическая работа №7

**Выполнил**:

студент группы К34211

Фисенко Максим Вячеславович

**Проверил**:

преподаватель практики, КТН

Назаров Михаил Сергеевич

Санкт-Петербург

2024

**Оглавление**

[**Введение** 3](#_Toc183968625)

[**Содержание отчета** 4](#_Toc183968626)

[**Задание 1. Проверка корректности работы Docker** 4](#_Toc183968627)

[**Задание 2. Создание лаборатории для тестирования и поиска уязвимостей** 5](#_Toc183968628)

[**Задание 3. Работа со сканером уязвимостей OpenVAS** 7](#_Toc183968629)

[**Вывод по работе** 11](#_Toc183968630)

# **Введение**

В данной практической работе необходимо было систематизировать знания и получить навыки по построению систем защиты информации, а также приобрести практические навыки в анализе систем защиты информации автоматизированных систем. В ходе выполнения практической работы необходимо было научиться находить «слабые» места в системах защиты автоматизированных систем.

При выполнении данной практической работы использовались системы следующих студентов:

* Семен Родионов;
* Глеб Шкода;
* Александр Хренов.

# **Содержание отчета**

## **Задание 1. Анализ системы Семена Родионова**

В качестве системы была использована ИТ-система школы.

В начале отчета кратко описана сама система, из описания понятно, что она из себя представляет. Затем сразу же перечислены все возможные роли пользователей систем, при этом разбиение на роли, как по мне, вышло довольно успешным: описаны все основные пользователи системы.

После этого были перечислены и описаны сегменты автоматизированный системы. Были выделены два сегмента: учебный и административный. Как по мне, в данной системе необходимо еще один сегмент – внутренний, в котором будут находиться рабочие станции сотрудников. В данной работе они находятся в административных и учебных сегментах, хотя, как по мне, стоило их вынести в отдельный.

Затем в работе описаны ОТСС и ВТСС выбранной автоматизированной системы. По моему мнению, ОТСС и ВТСС описаны верно, особенно в ВТСС подробно описаны все устройства, которые могут быть в школе.

Стоит отметить, что в работе я не обнаружил требования к сегментам. Были даны их описания, однако списка требования к каждому из сегментов мной обнаружено не было, вследствие чего можно сделать вывод, что по данному критерию будет -.

Далее в работе был выделен класс для каждого сегмента в соответствии с ФСТЭК. Для учебного сегмента был выбран класс 1Д, а для административного – 1Г.

Я считаю, что класс для учебного сегмента выбран не совсем верно, и тут больше подходит 1Г. Информация, циркулирующая в данном сегменте, не является общедоступной, поэтому класс 1Д, по моему мнению, тут не подойдет. Информация в этом сегменте хоть я не является тайной, но всё же и не считается за публичную и требует защиты, ведь любой желающий не должен иметь возможность смотреть оценки всех учеников, например.

Также я бы поспорил насчет класса для административного сегмента. В данном сегменте среди прочего циркулирует и конфиденциальная информация: например, в данном сегменте присутствует связь с госорганами. Данная информация является весьма чувствительной, поэтому я бы выбрал для этого сегмента класс 1В.

Далее в работе были подробно описаны все необходимые средства защиты информации, в том числе были указаны номера сертификатов. Итоговое графическое представление данной системы представлено на рисунке 1.

Изображение выглядит как текст, снимок экрана, диаграмма, дизайн

Автоматически созданное описание

Рисунок 1 - Итоговый вид системы

Так как схема строилась на основе описания, то вопросов именно к самой схеме нет, но, опять же, я бы выделил тут клиентские устройства в отдельный сегмент.

Таким образом, данной системе были выставлены оценки, представленные ниже в таблице 1. Стоит отметить, что оценки за некоторые из критериев является довольно спорными, поэтому в них я поставил +/-, а не выбрал что-то одно.

Таблица 1 - Оценка системы

|  |  |
| --- | --- |
| **Критерий** | **+/-** |
| Есть графическое представление системы | + |
| Есть описание назначения системы | + |
| Есть описание сегментов системы | +/- |
| Есть описание требований к классам АС | - |
| Описаны средства защиты информации | + |
| Указаны сертификаты на СЗИ | + |
| Есть графическое представление системы с подобранными средствами защиты | + |
| Есть описание мест установки СЗИ в системе | + |

В целом, я считаю, что моим коллегой была проделана большая работа, и, за исключением пары недостатков, у него получилось построить весьма хорошую систему защиты информации.

## **Задание 2. Анализ системы Глеба Шкода**

В качестве системы была использована информационная система интернет-магазина.

Сразу же можно заметить, что система описана максимально подробно: указаны данные, которые будут храниться в базе, цель системы, функциональные требования. Расписано, какие данные будут меняться автоматически, какие угрозы системе могут присутствовать.

Далее были перечислены ОТСС и ВТСС, где, как мне кажется, было допущено несколько ошибок. По моему мнению, системы логирования и резервные серверы стоит отнести к ОТСС, а не к ВТСС, ведь в них будет храниться конфиденциальная информация. Все остальные средства в перечне ОТСС, как мне кажется, описаны верно.

Затем в работе была расписана циркулирующая в системе информация, где, по моему мнению, было все расписано верно. После этого в работе было представлено графическое изображение системы (рисунок 2).

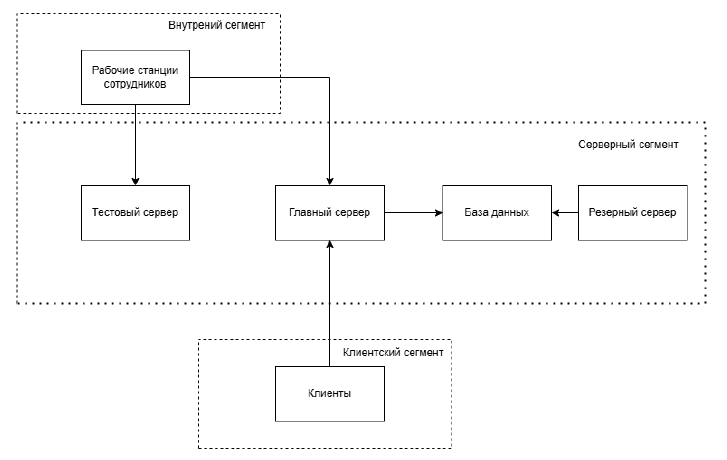


Рисунок 2 - Вид системы

По моему мнению, сегменты системы тут выделены верно, однако связи между серверами в серверном сегменте немного некорректны. Я думаю, что тестовый сервер должен быть связан с главным сервером для проведения интеграционных тестов, а также нагрузочных тестирования и для синхронизации конфигураций. Хоть и можно выделять тестовый сервер отдельно, всё-таки, мне кажется, что в данной ситуации он должен быть связан с главным сервером.

Также мне кажется, что рабочие станции сотрудников стоит разделить на каждую роль пользователя отдельно: должны быть отдельно администраторы системы и разработчики. Каждая из этих ролей будет связана с элементами серверного сегмента по-разному.

Еще в данной работе я не увидел подробного описания сегментов системы. Краткие описание присутствует, однако, как по мне, оно полностью не раскрывает суть назначения каждого из сегментов, и это можно в данной работе улучшить.

Затем были выявлены классы сегментов. Внутреннему сегменту был присвоен класс 3Б, а серверному – 1Д. Я согласен с присвоением внутреннему сегменту класса 3Б, однако, по моему мнению, серверному сегменту стоит дать класс 1Г, ведь там будут содержаться персональные данные, которые всё-таки надо защищать.

Далее были представлены средства защиты, к которым не были предоставлены номера сертификатов, что, как по мне, является ошибкой. В остальном со всеми средствами защиты я согласен, расписано всё было довольно подробно.

В выводе работы было составлено графические представление системы с подобранными средства защиты. Так как она фактически наследует предыдущее графическое представление, в ней есть те же недостатки, что и в предыдущей системе, однако средства защиты здесь проставлены, по моему мнению, правильно.

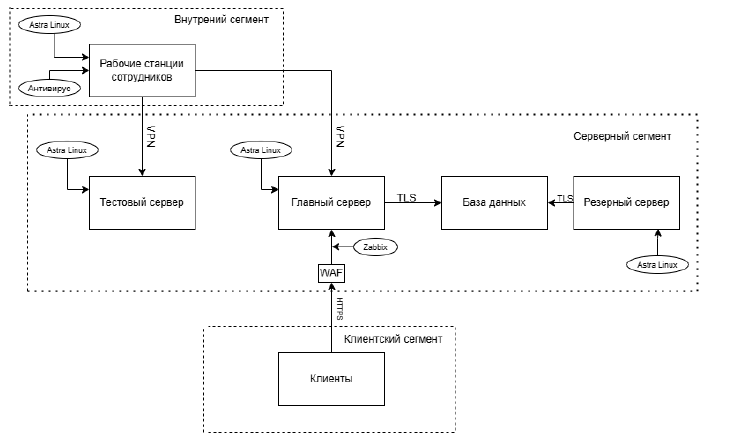


Рисунок 3 - Итоговый вид системы

В таблице 2 представлена итоговая оценка системы.

Таблица 2 - Оценка системы

|  |  |
| --- | --- |
| **Критерий** | **+/-** |
| Есть графическое представление системы | +- |
| Есть описание назначения системы | + |
| Есть описание сегментов системы | +- |
| Есть описание требований к классам АС | + |
| Описаны средства защиты информации | +- |
| Указаны сертификаты на СЗИ | + |
| Есть графическое представление системы с подобранными средствами защиты | + |
| Есть описание мест установки СЗИ в системе | + |

В целом, по моему мнению, мой коллега спроектировал хорошую систему, однако есть недостатки, которые можно исправить, чтобы система стала еще лучше.

# **Вывод по работе**

В результате выполнения данной лабораторной работы на персональном компьютере была развернута среда *OpenVAS*, которая просканировала контейнер с сервером *metasploit2* и обнаружила в нем уязвимости, показав каждую из них и отсортировав их список по степени опасности. Помимо *openvas*, в ходе выполнения работы был активно задействован *Docker*, а также утилиты *ping* и *ifconfig*. По результатам выполнения работы можно с уверенностью сказать, что цель практической работы была достигнута.