Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение

высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ

МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

им. Н.П. ОГАРЁВА»

(ФГБОУ ВО «МГУ им. Н.П. Огарёва»)

Факультет математики и информационных технологий

Кафедра фундаментальной информатики

**ЛАБОРАТОРНАЯ РАБОТА №2**

по дисциплине: Системы информационной безопасности предприятия

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОРПОРАТИВНЫХ СЕТЕЙ

Автор лабораторной работы А. Е. Конышев

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Преподаватель Е. Н. Гришанов

Оценка: \_\_\_\_\_\_\_

Саранск 2023

Цель работы: Описание корпоративной сети конкретного предприятия.

**Ход работы:**

Ознакомиться с теоретическим материалом.

Выполнить задания.

Задания:

Исходя из информации о специфике деятельности предприятия и структуры его локальной сети разработать политику сетевой безопасности (политику второго уровня) для указанного предприятия. Разработать настройки управляемых коммутаторов (выделение VLAN) и межсетевых экранов (таблица правил доступа) для предприятия с обоснованием этих настроек.

**Описание выполнения работы.**

Разработаем политику ЦДРиДО «Талантиум» на основе его локальной сети. Центр детского развития представляет собой 2-х этажное здание с небольшим количеством комнат. На первом этаже расположены административные комнаты: кабинет Директора, бухгалтерия, преподавательская, санузел, некоторое число комнат для цифрового обучения (компьютерные классы). На втором этаже расположена комната цифрового обучения, а также серверная комната, где в основном хранится и информация для работы этого центра.

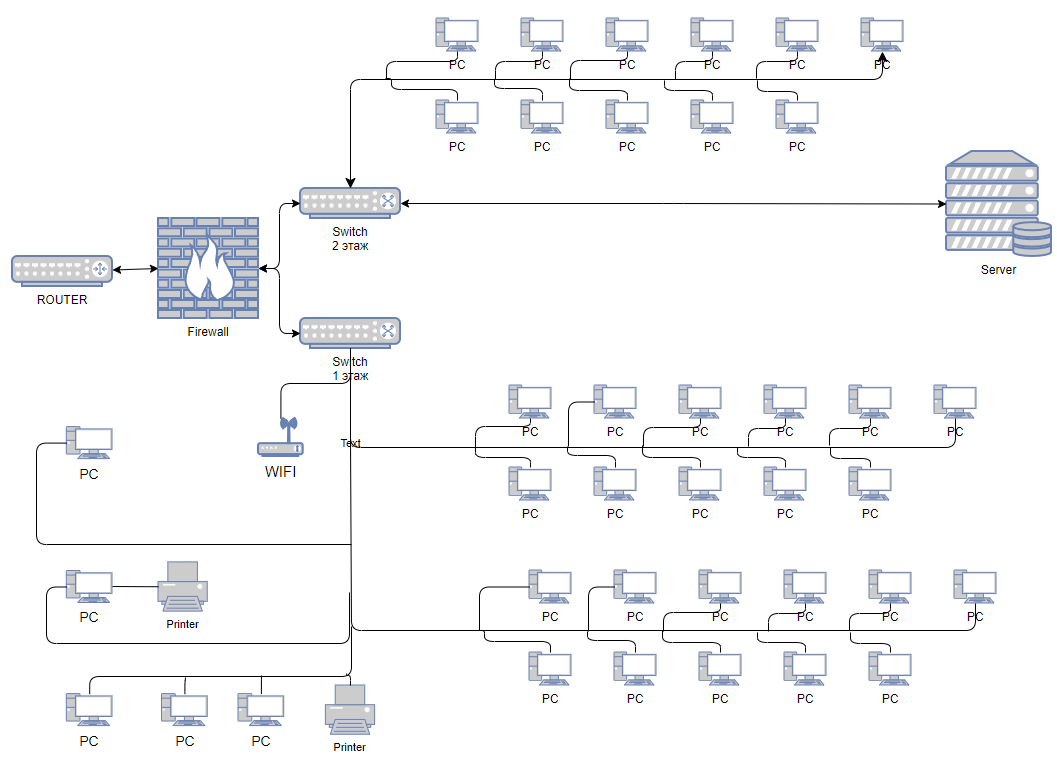


Рисунок 1 – Локальная сеть центра «Талантиум»

В центре образования основным элементом сети являются компьютеры, предназначенные для образования. Комнат с таким оборудованием во всем центре три: две на первом этаже и одна на втором, в каждой находится по 10 ПК для детей и 1 для преподавателя. Каждая такая комната предназначена только для образовательных целей и должна быть защищена от угроз, в первую очередь со стороны учеников. Для этих целей доступ в интернет происходит по белому списку брандмауэра. В таблице 1 содержится не исчерпывающий список правил брандмауэра. Ресурсы, необходимые для обучения будут добавляться по необходимости.

|  |  |  |  |
| --- | --- | --- | --- |
| Источник | Назначение | Протокол | Действие |
| Кабинет 1, кабинет 2, кабинет 3 | Talantium.ru | все | Разрешить |
| <https://stepik.org/ru> |
| [https://geekbrains.ru](https://geekbrains.ru/) |
| [http://www.lectarium.ru](http://www.lectarium.ru/) |
| [https://www.courser.org](https://www.courser.org/) |
| [https://otus.ru](https://otus.ru/) |
| [https://mirevo.ru](https://mirevo.ru/) |
| <https://lingualeo.com/ru> |
| [https://skillbox.ru](https://skillbox.ru/) |
| [https://openedu.ru](https://openedu.ru/) |
| [https://kursy.yandex.ru](https://kursy.yandex.ru/) |
| Microsoft.com |
| Java.com |
| Python.org |
| CodeBlocks.org |
| Все | Все | Запретить |

Таблица 1 – Часть правил брандмауэра

При подключении центра к сети Интернет используется брандмауэр, защищающий ресурсы центра от атак извне, и не допускающий использовать его ресурсы в целях злоумышленников. Но он не ограничивает доступ к сети для бухгалтерии, преподавательской и кабинету директора. Поэтому устройства, имеющие доступ из этих помещений, не содержатся в таблице. С другой стороны, доступ к запрещенным ресурсом ограничиваются провайдером.

Если произойдет ситуация, в которой со стороны сотрудников цента последуют противоправные действия, используются ПК центра, то таблица правил брандмауэра пополнится, дабы предотвратить подобные действия, и, конечно же, должно произойти расследование.