Министерство образования и науки

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Факультет инфокоммуникационных технологий

Отчет

по лабораторной работе № 1

**Исследование системы анализа рисков и проверки политики информационной**

**безопасности предприятия**

по дисциплине «Информационная безопасность в инфокоммуникационных системах»

**Выполнил: студент группы K4220**

**Кислюк Игорь Витальевич**

**Проверил: к.т.н., доцент И.В. Ананченко**

Санкт-Петербург

2018

## Задание.

* разработка и внедрение эффективных политик информационной безопасности;
* факторы, определяющие эффективность политики безопасности. Оценка риска;
* рекомендации по разработке и внедрению эффективных политик

## Индивидуальное задание.

* номер 10;
* компьютерная сеть предприятия включает в себя три подсети, доступ удаленных сотрудников по VPN, не используется PKI. Беспроводная сеть Wi-Fi поддерживается шифрование, тип безопасности WPA.

## Анализ данных

К факторам безопасности можно отнести возможность доступа посторонних лиц, отсутствие персональной авторизации сотрудников. Оценка текущих рисков настройки – данные могут быть скомпрометированы при получении доступа внутри сети, например, при посещении гостей.

Необходимо усилить контроль доступа для получения возможности работы внутри сети. Таким образом все сервера для работы – репозитории, сервера сборки и т. д. необходимо располагать за внутренней сетью с персональным доступом.

Среди эффективных политик безопасности можно выделить использование персональных ключей для подключения к рабочей сети Wi-Fi. Таким образом подключение без сертификата будет недоступным, тогда одну из подсетей необходимо выделить для гостевого Wi-Fi.

Три подсети могут сконфигурированы следующим образом. Главный роутер – 172.16.0.1 На следующий адресах располагаются внутренние почтовые сервера, сервера передачи данных, сервера для временного хранения паролей и т. д.

* 192.168.10.0 – Гостевая
* 172.16.0.0 – Рабочая
* 192.168.201.0 – Дополнительная рабочая при недостатке адресов.

Для доступа сотрудников по VPN используются токены для авторизации выдающиеся через сервер авторизации внутри компании.

## Вывод

Среди представленной конфигурации были найдены существующие уязвимости, которые могут помочь злоумышленникам скомпрометировать сотрудников и получить доступ к данным. Однако, для предотвращения такой ситуации следует внимательно относиться к доступности данных и проводить тренинги среди существующих сотрудников.