Тема выпускной квалификационной работы: Разработка политики информационной безопасности для АО «ЦИУС ЕЭС» - ЦИУС Юга, филиал в г. Пятигорске

Автор ВКР: Пугачёв Вячеслав Сергеевич

Научный руководитель ВКР: В.А. Рындюк, канд. техн. наук, доц. кафедры Информационных технологий, математики и средств дистанционного обучения

Сведения об организации-заказчике: АО «ЦИУС ЕЭС» - ЦИУС Юга, филиал в г. Пятигорске

Актуальность темы исследования: Достойный уровень защиты информации в современной организации может быть гарантирован только на основе комплексного подхода, начало которому - разработка и последующее внедрения политики безопасности. Поэтому разработка политики информационной безопасности организации является **актуальной,** первостепенной задачей.

Цель работы: разработка политики информационной безопасности для филиала АО «ЦИУС ЕЭС».

Задачи: характеристика Филиала АО ЦИУС ЮГА в г. Пятигорск; обзор правового регулирования мер по защите информации; постановка задачи по разработке политики информационной безопасности для АО «ЦИУС ЕЭС»; разработка основных положений политики ИБ для организации; выбор средств ЗИ с учетом предложенной политики безопасности; описание проекта практического применения выбранных средств..

Теоретическая значимость исследования нашей работы определяется актуальностью исследуемой темы и необходимостью подробного теоретического изучения проблемы обеспечения ИБ в организации; в анализе нормативных документов государственного и местного уровня по ИБ, анализа рынка современных средств ЗИ.

Практическая значимость работы определяется тем, что разработанная политика ИБ и описание применения средств защиты согласно ПИБ может быть практически внедрено в рассматриваемой организации.

Результаты исследования:. После произведенного анализа системы защиты информации сделан вывод о том, что необходимо внедрение электронного документооборота для оптимизации обрабатываемых и передаваемых данных, а также заменить устаревшие видеокамеры на более качественные Защита информации должна быть организована при помощи политики ИБ.

Рекомендации: Разработать политику ИБ, которая следующие разделы: Цели в области информационной безопасности. Задачи обеспечения информационной безопасности. Принципы обеспечения информационной безопасности. Ответственность за нарушение Политики информационной безопасности.

Кроме того, предложено ввести в действие некоторые Положения и Инструкции, регламентирующие деятельность персонала касательно ЗИ в информационной системе. Рекомендуется также усилить программно-аппаратную защиту организации: внедрить систему электронного

документооборота «Диадок» для оптимизации и защиты обрабатываемых и передаваемых данных; комплекс «Система защиты информации от НСД Dallas Lock 8.0-К» для защиты информации от несанкционированного доступа.

.