УДК 519.685

РАЗРАБОТКА СИСТЕМЫ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ НА ОСНОВЕ МОНИТОРНИГА И КОРРЕЛЯЦИИ

Гиоргобиани Давид

Грузинский университет им. Святого Андрея Первозванного Патриаршества Грузии

Аннотация

Данная публикация посвящена теоретическим и практическим аспектам разработки программно-аппаратного комплекса автоматизации обеспечения безопасности фунционирования организации путем защиты корпоратвной сети и рабочих мест сотрудников от несанкционированного доступа. Автором рассмартриваются вопросы полного технологического цикла по обеспечению безопасного функционирования организации – начиная формулировкой задач и кончая заключительными мерами, необходимыми для достижения цели.

Abstract

This publication is devoted to theoretical and practical aspects of the development of hardware and software automation security by protecting organizations operate correctly corporate network and workplaces of employees from unauthorized access. The author questions considered full technological cycle to ensure the safe operation of the organization - from the formulation of problems and ending with the final measures needed to achieve the goal.

Введение

По мере интенсификации использования сетевых и компьютерных технологий в деле обеспечения продуктивной работы организаций самого разного профиля, актаульность защиты рабочих мест от несанкционированного доступа становится все более и более актуальной. Более того, с уверенностью можно сказать, что на данный момент эта тематика становится критичной. Развитие технологий,позволяющих организовать эффективную защиту нормального функционирования организации происходит как области аппаратного обеспечения, так и сетевых технологий наряду с сопутствующим математическмим обеспечением. Повышение уровня интеллекта элементов, составляющих систему защиты, позволяет повысить уровень автоматизации системы защиты и, тем самым, ее эффективность.

Основная часть

Предлагается схема, в соответствии с которой вначале следует определить **задачи**, стоящие перед организацией по защите корпоративной сети и рабочих мест сотрудников. Эти задачи включают в себя:

1.Определение периметра корпоративной сети;
2.Определение IP адресов для рабочих мест;
3.Описание сетевых устройств;
4.Описание серверного ПО;
5.Описание системы администрирования пользователей
6.Описание правил политики безопасности пользователей
7.Определение правил политики безопасности для сетевого оборудования и сотрудников
8.Подготовка среды для мониторинга корпоративной сети и сотрудников
9.Определение инцидентов и создание правил для реагирования

10. Создание правил для корреляции
11. Определение и подготовка группы для мониторинга и администрирования

После полного описания вышеприведенных задач, уже можно сформулировать конкретные цели, достижение которых обеспечивает защиту корпоративной сети и рабочих мест сотрудников. После чего следует определить ключевые факторы риска, устранение которых является предметом первой необходимости. И лишь после этого определяются меры для достижения поставленных целей, включающие:

1. Меры организационного плана определенные в соответствии с пунктами 5, 6 и 7, вышеприведенных задач.
2. Меры технологического плана: аппаратно – сетевого характера, в соответствии с пунктами 1–3, 8 вышеприведенных задач, программного характера, в соответствии с пунктами 4, 8–10, а также системного характера – в соответствии с пунктом 11.

Заключение

Как легко заметить, предлагаемая схема имеет весьма обобщенный характер и может быть использована для организаций самого разного профиля. Выбор конретных решений и используемых технологий зависит от характерстик организации (размеры, финансы, приоритеты и др.). В данный момент развитие предлагаеиой концепции идет в направлении автоматизации настройки данной схемы на конкретную организацию, путем формализации характеристик этой организации в разрезе вышеприведенных задач. В будущем представляет интерес разработка целевой технологии, обеспечивающей поддержку функционирования организации, включающей защиту корпоративной сети и рабочих мест сотрудников.

Список использованных источников:

1. Кияев В., Граничин О. Безопасность информационных систем. ИНТУИТ, 2016.
2. Мэйволд Э. Безопасность сетей. ИНТУИТ, 2016.