Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.056

УЧАЕВ
Никита Александрович

МЕТОДИКА ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ ПЕРЕДАВАЕМЫХ В КОРПОРАТИВНЫХ СЕТЯХ ПРЕДПРИЯТИЯ

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
кандидат технических наук, доцент
Петров Сергей Николаевич

Минск 2017

ВВЕДЕНИЕ

Возрастающее из года в год количество кибератак на корпоративные сервисы выводит вопросы защиты информации на первый план. В сфере обеспечения защиты корпоративных сервисов существует масса нормативной документации от профильных структур. Не глядя на это, количество атак не перестаёт расти, что говорит о том, что предлагаемые методики либо не соответствуют требованиям настоящего времени, либо не применяются вовсе по различным причинам

В качестве решения сложившейся ситуации можно рассмотреть создание новой методики защиты информации в корпоративных информационных системах. Данная методика должна быть практико-ориентированной и должна позволять специалистам любого уровня квалификации безопасно устанавливать и обслуживать корпоративные сервисы. Архитектура методики должна позволять вести её разработку и развитие силами сообщества высококлассных специалистов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Предложенная в диссертационной работе методика автоматизирует применение рекомендаций института SANS, изложенных в документах «CIS Critical Security Controls» и «CIS Security Benchmarks», а также снижает затраты на выполнение некоторых положений, изложенных в приказе ОАЦ номер 62.

Цель и задачи исследования

Целью диссертационной работы является разработка методики построения системы защиты данных передаваемых в корпоративных сетях предприятия.

Поставленная цель работы определяет следующие основные задачи:

1. Провести обзор и анализ имеющихся методик, рекомендаций и нормативных документов.
2. Разработать архитектуру конечной методики.
3. Рассмотреть применение методики в различных сценариях.

Апробация результатов диссертации

Материалы исследований, используемые при написании диссертации, докладывались и обсуждались 12-й международной молодежной научно-технической конференции (Севастополь, 14-18 ноября 2016 г.).

Опубликованность результатов диссертации

Изложенные в диссертации основные положения и выводы опубликованы в 2 печатных работах. В их числе 1 статья в сборниках материалов конференций.

Структура и объем диссертации

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трех глав, заключения и библиографического списка. Общий объем диссертации – 49 страниц, работа содержит 20 рисунков, библиографический список включает 18 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В **общей характеристике работы** сформулированы ее цель и задачи, показана связь с приоритетными направлениями научных исследований.

Во **введении** рассмотрено состояние проблемы необходимости совершенствования методов и средств защиты информации, применяемых в корпоративных информационных системах, определены основные требования к конечной системе и вектор ещё дальнейшего развития.

В первой главе приведен обзор структурных компонентов, возможных угроз и методов защиты корпоративных информационных систем, а также выбраны ключевые положения из нормативных источников и обусловлен выбор направлений деятельности при реализации методики защиты информации.

Во второй главе рассмотрены основные программные компоненты, являющиеся частью разрабатываемой методики, процесс разработки компонентов методики, а также различные сценарии их применения.

В третей главе представлены результаты применения разработанных методик в различных сценариях. Обусловлен выбор различных

вспомогательных программных решений для обеспечения комплексной защиты информационных систем предприятия.

В **приложении** приведен графический материал для защиты магистерской диссертации.

ЗАКЛЮЧЕНИЕ

В процессе выполнения работы были рассмотрены имеющиеся нормативные постановления и рекомендации и выбраны оптимальные, для построения конечной методики, удовлетворяющей поставленным требованиям. Был проанализирован широкий спектр программных продуктов, использование которых позволило бы обеспечить выполнение поставленной перед методикой задач.

В тексте работы рассмотрены типовые сценарии атак на корпоративный сектор, уязвимые компоненты информационных систем и методика эксплуатации различных уязвимостей. Предложены сценарии и программные методы для повышения защищённости конечного решения.

Фреймворк, разработанный в процессе написания работы, представляет собой набор сценариев Ansible и специальных скриптов, расположенный в публичном Git-репозитории. В дальнейшем, сценарии могут разрабатываться совместно, силами сообщества высококвалифицированных инженеров.

Описан сценарий применения предприятиями разработанной методики., возможность применения инфраструктуры публичных и частных репозиториев конфигураций и методика их разработки и сопровождения.

Разработанная методика обеспечения защиты информации способна развиваться в дальнейшем силами сторонних специалистов, а неё применение позволит обезопасить корпоративные сервисы и сети.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Построение гибридной отказоустойчивой корпоративной телефонной сети / Н.А. Учаев, С.Н. Петров и др.// Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы международного научно-технического семинара. В 2 ч. Ч 2 (Минск, апрель-декабрь 2016 г.). – Минск: БГУИР, 2016. –С. 79-84.

2. Uchaev N.A., Smirnova Z.D., Petrov S.N. Application of IP-telephony as a secure alternative for GSM communication. Современные проблемы радиоэлектроники и телекоммуникаций “РТ – 2016” : материалы 12-й

международной молодежной науч.-техн. конф., Севастополь, 14-18 ноября 2016 г.. – С. 206-207.