Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.056

БУКШТЫНОВА
Анна Игоревна

ЗАЩИТА ВЕБ-СЕРВЕРА ОРГАНИЗАЦИИ ОТ АТАК

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

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

Научный руководитель
доктор технических наук, профессор
Борботько Тимофей Валентинович

Минск 2017

ВВЕДЕНИЕ

В настоящее время развитие информационных технологий и увеличение информационного пространства оказывает значительное влияние на современное общество, а также все виды человеческой деятельности, связанные с обработкой и хранением информации.

Глобальная сеть Интернет является неотъемлемой частью жизни человека. Её пропускная способность постоянно возрастает, что позволяет создавать многопользовательские приложения для работы по всему миру. Такие системы широко используются в областях здравоохранения, связи, кредитования, военных подразделений и многих других.

Веб-сайты представляют собой мощный инструмент, с помощью которого правительственные, общественные и коммерческие организации обмениваются информацией. В связи с этим постоянно увеличивается количество потенциальных злоумышленников, пытающихся завладеть конфиденциальной информацией. Опасностью для надежной защиты информационных ресурсов являются сетевые атаки. Поэтому одной из приоритетных задач выступает предотвращение сетевых атак в области защиты информационных систем.

Большинство современных систем имеют распределенную структуру, в основе которой лежит использование сетевых технологий. И обеспечение надежного доступа к таким системам зависит от способности противостоять действиям злоумышленника, которые направлены как на нарушение работы самой сети, так и информационной системы, функционирующей в ее рамках. Одним из наиболее опасных видов злонамеренных действий являются сетевые атаки. С каждым годом количество сетевых атак продолжает расти, методы, которыми пользуются злоумышленники, постоянно развиваются и совершенствуются, от одиночных попыток взлома переходят к корпоративным атакам.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых

Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке архитектуры системы защиты веб-сервера организации от атак.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать уязвимости и современные подходы для защиты веб-серверов.
2. Проанализировать различные средства и методы защиты веб-сервера от атак.
3. Разработать архитектуру системы защиты веб-сервера и организационно-технические мероприятия.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XV Белорусско-российской научно-практической конференции «Технические средства защиты информации» (Минск, 2017).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликована 1 работа, в том 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 и заключения, библиографического списка и приложений. Общий объем диссертации – 57 страниц, работа содержит 10 рисунков, библиографический список включает 30 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено состояние проблемы необходимости совершенствования методов и средств защиты, применяемых в информационных системах, определены основные направления исследований, а также дается обоснование актуальности темы диссертационной работы.

В **общей характеристике работы** сформулированы ее цель и задачи, показана связь с приоритетными направлениями научных исследований, приведена апробация результатов диссертации и их опубликованность.

В первой главе рассматриваются современные клиент-серверные технологии, описывается трехуровневая модель локальной сети на основе оборудования компании *D-Link* и *Cisco*, представлена модель взаимодействия клиента и сервера, рассмотрены наиболее популярные *HTTP*-методы, такие как *GET* и *POST*.

Во второй главе приведен анализ наиболее популярных уязвимостей веб-серверов *OWASP* TOP-10, рассмотрены разнообразные взломщики паролей, проанализированы различные уязвимости веб-серверов и организации, не только со стороны информационных систем, но и сотрудников компании, рассмотрены наиболее распространенные техники социальной инженерии, а также современные подходы в обеспечении защиты веб-серверов от атак.

В третей главе проанализированы возможные атаки на банковскую систему и методы противодействия этим атакам, представлены результаты построения архитектуры системы защиты банковской организации, разработки комплекса организационно-технических мероприятий для обеспечения защиты веб-сервера от атак.

ЗАКЛЮЧЕНИЕ

В магистерской диссертации решена актуальная задача, имеющая практическое применение. Сущность её заключается защите веб-сервера организации от атак, используя разработанную систему защиты и применяя организационно-технические мероприятия.

В ходе выполнения магистерской диссертации, поставленные цели были достигнуты в полном объеме. Произведен анализ уязвимостей веб-серверов на основании *OWASP TOP*-10 и наиболее популярных атак на веб-сервер, проанализированы современные подходы в обеспечении защиты веб-серверов от атак, разработана архитектура системы защиты и организационно-технические мероприятия.

В результате выполнения магистерской диссертации разработана архитектура системы защиты организации. Данная система включает в себя систему антивирусной защиты, *IPS*-систему, использование МСЭ на обеих сторонах *DMZ*.

Результаты магистерской диссертации были представлены на XV Белорусско-российской научно-технической конференции «Технические средства защиты информации» 6 июня 2017 года.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Kahtan Hussein. Software solution for vulnerability detection / Kahtan Hussein, Momoh Angelo, Bukshtynova A.I. // Технические средства защиты информации : материалы XV Белорусско-российской науч.-техн. конф., Минск, 6 июня 2017 г. / БГУИР ; редкол. : Т. В. Борботько [и др.]. – Минск, 2017. – 116 с.