

Министерство образования Республики Беларусь  
Учреждение образования  
«Белорусский государственный университет  
информатики и радиоэлектроники»

УДК 004.056.5

**ФЕДОРОВИЧ**  
**Полина Сергеевна**

**ЗАЩИТА SSL СЕРВЕРА ПРОЦЕССИНГОВОГО ЦЕНТРА ОТ АТАК**

**АВТОРЕФЕРАТ**

на соискание степени магистра технических наук

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

Научный руководитель  
Борботько Тимофей Валентинович  
доктор технических наук, профессор

Минск 2017

## **ВВЕДЕНИЕ**

В современных условиях экономического роста вместе со стремительным развитием безналичных платежей и популяризацией систем дистанционного обслуживания также увеличилось количество атак, направленных на хищение денежных средств с использованием платежных карт. Бизнес-структуры банковской сферы уделяют наибольшее внимание решению данной проблемы, концентрируя свои усилия на технических аспектах защиты персональных данных.

В системах удаленного банковского обслуживания для обеспечения конфиденциальности передаваемых данных используются средства, обеспечивающие их шифрование. Наиболее широко распространен в таких системах протокол SSL, техническая реализация которого основана на использовании SSL-сервера. Решение о применении SSL сервера исходит из важности обеспечения конфиденциальной передачи данных в сети Интернет. В сфере бизнеса применение SSL сертификатов гарантирует клиентам, что риск утечки информации при ее передаче через открытые сети исключен. Защита SSL сервера от атак и построение защищенной архитектуры прохождения трафика является приоритетной задачей процессингового центра.

## **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 SSL сервера процессингового центра от атак.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать угрозы информационной безопасности для SSL серверов.
2. Проанализировать методы и средства защиты хостов сети от атак.
3. Разработать архитектуру системы защиты SSL сервера процессингового центра от атак.

### **Апробация результатов диссертации**

Основные положения и результаты диссертации обсуждались на XII Международной научно-практической конференции «Управление информационными ресурсами» (Минск, 2016).

### **Опубликованность результатов диссертации**

По результатам исследований, представленных в диссертации, опубликовано 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 — 90 страниц, работа содержит 34 рисунка, библиографический список включает 37 наименований.

## **КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ**

Во **введении** рассмотрено состояние проблемы необходимости совершенствования методов и средств защиты, применяемых в системах дистанционного банковского обслуживания, 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 роль процессингового центра в сфере безналичных платежей, алгоритм обработки интернет-платежей, принцип работы POS-терминалов, а также анализируются требования международных

платежных систем и локальных законодательных актов к процессинговым центрам.

**Во второй главе** приведен анализ состояния технологии SSL на текущий момент: технические аспекты, терминология, развитие, использование протокола в современных информационных системах, принцип работы; представлен обзор состояния безопасности SSL протокола: виды возможных атак, обзор уязвимостей, реализуемых атак на базе этих уязвимостей и методов защиты.

**В третьей главе** представлены результаты построения архитектуры системы защиты SSL сервера, разработки комплекса мероприятий для обеспечения защиты сервера от атак, а также произведен подбор оптимальной настройки конфигурации SSL-сервера на примере программного обеспечения Radware Appdirector.

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

## **ЗАКЛЮЧЕНИЕ**

1. Проведена систематизация знаний для понимания структуры, особенностей и самого процесса обработки транзакционного трафика: развитие процессинговых платежей, роли процессинговых организаций, принцип работы POS-терминалов, эквайринга, клиринга; произведен анализ требований международных платежных систем к процессинговым центрам, а также обзор законодательной базы Республики Беларусь, касательно персональных данных.

2. Проведено исследование технических аспектов SSL технологии: использование протокола в современных информационных системах, применение SSL-сертификатов, принцип работы SSL; проанализированы уязвимости SSL, реализуемые атаки на базе этих уязвимостей и методы защиты SSL-серверов от атак.

3. Разработаны основные принципы организации защищенного подключения POS-терминалов к процессинговому центру, на основе которых спроектирована архитектура системы защиты, представляющая собой непрерывный контур инспекции данных на каждом этапе прохождения пакета.

4. Разработан комплекс организационных и технических мероприятий, соблюдение которых позволит не только снизить риски и защитить SSL-сервер от атак, но и поддерживать в актуальном состоянии всю систему процессинга, обеспечить отказоустойчивую систему.

5. По результатам разработанного комплекса мероприятий произведен подбор оптимальной настройки конфигурации на примере продукта Radware AppDirector.

## **СПИСОК ОПУБЛИКОВАННЫХ РАБОТ**

1-А. Федорович, П.С. Принципы организации защищенного подключения POS-терминалов к процессинговому центру / П.С.Федорович // Управление информационными ресурсами: материалы XIII Междунар. науч.-практ. конф., Минск, 9 дек. 2016 г. – Минск: Акад. упр. при Президенте Респ. Беларусь, 2016 – с. 203

Библиотека БГУИР