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

УДК 654.1:004.056

Жукевич
Андрей Фёдорович

Методика оперативного аудита информационной безопасности телекоммуникационных сетей и устройств

АВТОРЕФЕРАТ

магистерской диссертации на соискание степени магистра технических наук

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

_____

Научный руководитель

Маликов Владимир Викторович
кандидат технических наук, доцент

_____

Минск 2019

ВВЕДЕНИЕ

В настоящее время в мире и в частности Республике Беларусь активно строятся/используются телекоммуникационные сети и устройства, которые позволяют осуществлять доступ к информационным системам и ресурсам объектов различных категорий.

Возможности быстрой коммуникации используются гражданами для реализации личных интересов, а также организациями различных форм собственности при осуществлении финансово-экономической деятельности.

Массовое внедрение информационных систем и технологий электронных платежей, а также наличие уязвимостей в таких системах, привлекает специалистов криминальной сферы деятельности, что приводит к значительному росту совершаемых киберпреступлений.

Существует острая потребность в повышении эффективности построения и управления системой защиты информации телекоммуникационных сетей и устройств, а также разработки методик проведения оперативного аудита таких систем.

Таким образом, необходимость проведения данного исследования обусловлена массовым внедрением информационных систем и технологий электронных платежей, а также появлением новых угроз безопасности в таких системах, связанных с возможностью реализации злоумышленниками уязвимостей, результаты которых негативно влияют на обеспечение информационной безопасности организаций различных форм собственности.

Целью работы является разработка методики оперативного аудита информационной безопасности телекоммуникационных сетей и устройств.

Проводимые в рамках настоящей диссертации исследования позволяют решить важную научную задачу, связанную с эффективным обеспечением защиты телекоммуникационных сетей и устройств.

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 методики оперативного аудита информационной безопасности телекоммуникационных сетей и устройств.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. собрать и проанализировать статистические данные по системам информационной безопасности, а также по моделям и методам проведения оперативного аудита телекоммуникационных сетей и устройств;
2. разработать методику повышения эффективности построения систем информационной безопасности телекоммуникационных сетей и устройств;
3. разработать методику оперативного аудита информационной безопасности телекоммуникационных сетей и устройств.

Апробация результатов диссертации

Методика оперативного аудита была опробована на системе информационной безопасности типовой телекоммуникационной сети.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 работы, в том числе 2 тезиса докладов в сборнике материалов конференции.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, четырёх глав, заключения и библиографического списка. Общий объем диссертации 57 страниц, 30 наименований в библиографическом списке.

Во введение приводится обоснование актуальности работы.

Первая глава носит обзорный характер. В ней приводится описание угроз и уязвимостей информационной безопасности телекоммуникационных сетей и устройств, статистические данные по нарушению систем защиты, по методам и средствам обеспечения информационной безопасности в телекоммуникационных сетях и устройствах, по моделям и методам проведения оперативного аудита систем информационной безопасности в телекоммуникационных сетях и устройствах.

Вторая глава посвящена повышению эффективности построения систем информационной безопасности телекоммуникационных сетей и устройств. В ней приводятся угрозы ИБ при построении систем информационной безопасности телекоммуникационных сетей и устройств и типовые критерии при оценке эффективности построения систем информационной безопасности телекоммуникационных сетей и устройств, которые позволяют противостоять данным угрозам. Также во второй главе разрабатывается методика повышения эффективности построения систем информационной безопасности телекоммуникационных сетей и устройств.

В третьей главе описывается разработка методики оперативного аудита информационной безопасности телекоммуникационных сетей и устройств, которая позволяет оценить уровень защищённости телекоммуникационной сети и устройств по набору типовых показателей и критериев.

В четвёртой главе описывается апробация методики оперативного аудита на системе информационной безопасности типовой телекоммуникационной сети и устройствах.

В заключении сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

В рамках данной работы были рассмотрены угрозы и уязвимости информационной безопасности в телекоммуникационных сетях и устройствах, проанализированы статистические данные по нарушению систем защиты, а также проанализированы существующие подходы проведения аудита информационной безопасности телекоммуникационных сетей и устройств.

Рассмотрено наиболее популярное ПО для оценки эффективности систем информационной безопасности.

На основе результатов выполненного анализа разработана методика повышения эффективности построения систем информационной безопасности телекоммуникационных сетей и устройств, позволяющая проводить комплексную оценку на основе разработанных типовых критериев качества проектирования и внедрения с учетом угроз при построении таких систем, а также методика оперативного аудита систем информационной безопасности телекоммуникационных сетей и устройств, основанная на анализе угроз системы информационной безопасности, позволяющая провести оценку уровня защищенности телекоммуникационных сетей и устройств с принятием мер по снижению рисков нанесения потенциального ущерба их владельцам.

Разработаны критерии оценки уровня защищенности телекоммуникационных сетей и устройств на основе 9-ти комплексных критериев (контроль доступа, осведомлённость и обучение персонала, аудит и отчётность, оценка безопасности, управление конфигурацией, планирование непрерывного управления, идентификация и аутентификация, реагирование на инциденты, обслуживание системы), включающих 47 частных критерия.

Преимуществом разработанной методики является её универсальность, что позволяет проводить аудит информационной безопасности любой телекоммуникационной сети и устройств.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1А. Жукевич, А.Ф. Методика аудита безопасности информационных систем // А.Ф. Жукевич, В.В. Маликов // Управление информационными ресурсами: материалы XIV–ой междунар. НПК, Минск, 20 декабря 2017 г. / редкол.: М.Г. Жилинский [и др.]. – Мн.: Акад. упр. при Президенте Респ. Беларусь, 2017. – С. 169 – 171.

2А. Жукевич, А.Ф. Тестирование сетевых сканеров уязвимостей: Openvas, Nessus, Rapid7 Nexpose // Тезисы докладов XVI Белорусско-российской научно–технической конференции, Минск, 5 июня 2018 г. / редкол.: Т.В. Борботько [и др.]. Минск: БГУИР, 2018. – С. 39 – 40.

3А. Жукевич, А.Ф. Обход биометрической аутентификации в мобильных приложениях / О.В. Бородюк, А. Ф. Жукевич // Современные средства связи: материалы XXIII Междунар. науч.-техн. конф., 18–19 окт. 2018 года, Минск, Респ. Беларусь; редкол.: А. О. Зеневич [и др.]. – Минск: Белорусская государственная академия связи, 2018. – С. 189.