



ВЕГА

АКЦИОНЕРНОЕ ОБЩЕСТВО «КОНЦЕРН РАДИОСТРОЕНИЯ «ВЕГА»
ФИЛИАЛ В Г. САНКТ-ПЕТЕРБУРГЕ
JOINT-STOCK COMPANY «RADIO ENGINEERING CORPORATION «VEGA»
BRANCH IN ST. PETERSBURG

Экз. № 1

Председателю диссертационного совета
Д.002.199.01
Юсупову Рафаэлю Мидхатовичу

199178, Санкт-Петербург
14 линия, 39,
Федеральное государственное бюджетное
учреждение науки Санкт-Петербургский
институт информатики и автоматизации
Российской академии наук

Отзыв

на автореферат диссертации ДОЙНИКОВОЙ Елены Владимировны на тему
«Оценка защищенности и выбор защитных мер в компьютерных сетях
на основе графов атак и зависимостей сервисов»,
представленной на соискание ученой степени кандидата технических наук
по специальности 05.13.19 – «Методы и системы защиты информации,
информационная безопасность»

Область обеспечения информационной безопасности активно развивается, особенно в последние годы. Тем не менее, не смотря на существующие наработки, по-прежнему осуществляется множество успешных атак на компьютерные сети. В текущей ситуации, когда нарушение безопасности компьютерной сети может нанести предприятию серьезный урон, актуальность обеспечения информационной безопасности, в том числе, оценки защищенности компьютерной сети и выбора защитных мер, не вызывает сомнений. Таким образом, задача разработки модельно-методического аппарата для оценки защищенности компьютерных сетей и выбора защитных мер, поставленная в диссертационном исследовании, является актуальной.

В работе представлены следующие результаты:

1. Комплекс показателей защищенности компьютерных сетей на основе графов атак и зависимостей сервисов.
2. Методика оценки защищенности компьютерных сетей на основе графов атак и зависимостей сервисов.
3. Методика выбора защитных мер на основе графов атак и зависимостей сервисов.
4. Архитектура и программная реализация системы оценки защищенности компьютерных сетей и выбора защитных мер на основе предложенных методик.

Новизна результатов состоит в способе классификации входных данных, применяемых для оценки защищенности и выбора защитных мер, совокупности используемых моделей, показателей и алгоритмов оценки, и взаимосвязях между ними, позволяющих на основе доступных данных получать оценку защищенности и выбирать рациональные с точки зрения эффективности реагирования и стоимости защитные меры на этапах проектирования и эксплуатации системы.

Полученные результаты могут применяться при формировании систем обеспечения информационной безопасности предприятий.

Обоснованность и достоверность результатов подтверждается рядом экспериментов по оценке защищенности и выбору защитных мер для сетей различного размера и различных компьютерных атак, а также успешной апробацией на российских и международных научных конференциях. Основные результаты исследования опубликованы в журналах из списка ВАК, а также в журналах, индексируемых в международных базах Scopus и Web Of Science.

Замечания по автореферату:

1. В реальных системах практически никогда не известны точные значения параметров атакующих действий, таких как вероятности конкретных действий и состояний атакующего, вероятность компрометации узлов графа и т.п. Поэтому возникает вопрос: насколько в предлагаемой методике оценки защищенности неточен вычисленный уровень защищенности компьютерной сети?

2. Отсутствуют оценки сложности реализации предлагаемых технических решений по обеспечению безопасности компьютерных сетей.
3. В автореферате не приведено ни одного численного значения показателей защищенности, что затрудняет оценку степени достигнутого в работе повышения защищенности компьютерных сетей.

Указанные замечания не снижают научной ценности заявленных результатов.

Рассматриваемое диссертационное исследование соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» и требованиям п. 9 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства РФ № 842 от 24 сентября 2013 г., обладает актуальностью и новизной, и является завершенной квалификационной научной работой.

Соискатель **ДОЙНИКОВА Е.В.** заслуживает присуждения ей степени кандидата технических наук по специальности 05.13.19.

Ведущий научный сотрудник филиала АО «Концерн радиостроения «Вега» в г. Санкт-Петербурге доктор технических наук, профессор
ОКОВ Игорь Николаевич

Сведения о составителе отзыва:

Оков Игорь Николаевич, доктор технических наук, профессор, ведущий научный сотрудник филиала «Концерн радиостроения «Вега» в г. Санкт-Петербурге.

Почтовый адрес: ул. Академика Павлова, д. 14а, г. Санкт-Петербург, 197376.

Тел.: 89213238999

Электронная почта: okow1@mail.ru

Подпись руки И.Н. Окова удостоверяю.

Директор Филиала АО «Концерн радиостроения «Вега» в г. Санкт-Петербурге
кандидат технических наук **ПРИЩЕПА Юрий Владимирович**

«12» мая 2017

ПРИЩЕПА Юрий Владимирович