

УТВЕРЖДАЮ

И.о. директора ФГБУН
Институт проблем управления
им. В.А. Трапезникова РАН



Губко М.В.

ОТЗЫВ

ведущей организации на диссертационную работу Е.А. Мартьянова
«Исследование и разработка методик оценки защищенности
информационных объектов от потенциальных нарушителей»,
представленной на соискание ученой степени
кандидата технических наук по специальности
05.13.19 «Методы и системы защиты информации, информационная
безопасность»

Актуальность темы диссертационной работы

С развитием информационных технологий все более актуальной является проблематика обеспечения информационной безопасности. Эта проблематика вызывает большой интерес с теоретической и практической точек зрения. Существует большое количество моделей и программных средств, связанных с обеспечением информационной безопасности различных информационных систем и сетей.

В диссертационной работе Е.А. Мартьянова рассматриваются те угрозы информационной безопасности организаций, которые обусловлены деятельностью инсайдеров – сотрудников организации, обладающих легальным доступом к ее информационным ресурсам, но использующих эти ресурсы в ущерб компании. Инсайдеры представляют серьезную угрозу, и разработка методов противодействия им представляется актуальной задачей.

Новизна проведенных исследований и полученных результатов

В представленной на отзыв диссертационной работе новыми являются следующие результаты.

1. Модели поведения обычного пользователя и инсайдера в информационной системе организации, позволяющие использовать теорию запретов вероятностных мер для их различения.

2. Метод выявления потенциального инсайдера из множества пользователей (сотрудников организации), основанный на выявлении факта сбора не обусловленной должностными обязанностями информации. Метод гарантирует отсутствие ложных срабатываний и обеспечивает успешное выявление инсайдера за конечное время.

3. Программное средство имитационного моделирования работы пользователя с данными, позволяющее получать экспериментальные результаты применения статистических методов для выявления инсайдера.

Степень обоснованности и достоверности научных результатов, выводов и рекомендаций

Научные результаты, выводы и рекомендации, сформулированные в диссертационной работе, достаточно обоснованы и достоверны. Доказательством этому является использование апробированных методов теории вероятностей, математической статистики, теории множеств, имитационного моделирования.

Теоретическая и практическая значимость

Теоретическое значение диссертации заключается в разработке научном обосновании моделей и методов, позволяющих противостоять нарушениям информационной безопасности организации со стороны ее сотрудников.

Практическое значение работы состоит в возможности использования разработанных моделей и методов для совершенствования программного обеспечения для выявления нарушений информационной безопасности.

Соответствия требованиям, предъявляемым к диссертациям

Рассматриваемая диссертационная работа представляет собой законченное научное исследование, в котором разработаны и исследованы модели и методы выявления внутриорганизационных угроз информационной безопасности. Работа написана ясным, технически грамотным языком. Основные положения диссертации изложены в шести научных работах, в том числе в четырех статьях в рецензируемых журналах. Автореферат достаточно полно отражает содержание работы.

Замечания по содержанию работы

1. Целенаправленное воздействие инсайдера является, по сути, ситуацией противоборства. В частности, инсайдер пытается добиться своих целей (воровство интеллектуальной собственности и т.п.) и при этом избежать обнаружения. Однако в работе не рассматривается вопрос о возможных действиях инсайдера в ответ на предлагаемую стратегию его выявления (если стратегия станет ему известна).

2. На сс. 71-72, идет речь о том, что требование присутствия в защищаемой системе реального инсайдера для проверки методов его выявления является трудновыполнимым. Но это не совсем так: для тестирования методов выявления роль инсайдера может выполнять, например, сотрудник организации.

3. В работе без обсуждения предполагается, что важные (представляющие ценность) для организации данные являются важными и для инсайдера (см., напр., с. 85). Однако, вообще говоря, ценность данных для организации и для инсайдера может быть различной.

4. Замечена некоторая небрежность в использовании математической терминологии («дробное число» на с. 78) и обозначений (множество натуральных чисел обозначено разными буквами на страницах 50 и 52), имеются опечатки (напр., пропущена закрывающая скобка на с. 56).

Рекомендации по использованию результатов диссертации

Результаты диссертационной работы рекомендуется использовать в научно-исследовательской работе по проблемам информационной безопасности в научно-исследовательских институтах РАН, в образовательных организациях, а также в практической работе по обеспечению информационной безопасности в организациях, эксплуатирующих корпоративные информационные системы.

Заключение

Диссертация Мартьянова Евгения Александровича является законченной квалификационной научно-исследовательской работой, содержащей новые научные и практические результаты, связанные с решением актуальной задачи. Высказанные в настоящем отзыве замечания не снижают общего высокого научного и практического значения представленной диссертационной работы. Работа соответствует специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» и требованиям ВАК при Минобрнауки России, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор Мартьянов Евгений Александрович заслуживает присвоения искомой ученой степени.

Отзыв составлен доктором физико-математических наук, заведующим лабораторией Чхартишвили А.Г., обсужден и одобрен на расширенном заседании лабораторий № 57 «Активных систем» и № 79 «Сложных сетей» ИПУ РАН 21 февраля 2019 г. (протокол № 3).

Доктор физико-математических наук,
главный научный сотрудник,
заведующий лабораторией № 79 «Сложных сетей»
ФГБУН Институт проблем управления им. В.А. Трапезникова
Российской академии наук (ИПУ РАН),
специальность 05.13.01 – «Системный анализ, управление и обработка информации (в отраслях информатики, вычислительной техники и автоматизации)».

Тел.: +79037749537, e-mail: sandro_ch@mail.ru.

/ А.Г. Чхартишвили /

Сведения об организации.

Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В.А. Трапезникова Российской академии наук.
Почтовый адрес: Россия, 117997, Москва, ул. Профсоюзная, д.65.
Тел.: +7 (495) 334-89-10, e-mail: dan@ipu.ru.

