

ОТЗЫВ

официального оппонента к.т.н., доцента Малёшиной Людмилы Михайловны на диссертацию и автореферат диссертации Черникова Романа Сергеевича на тему «Модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов», представленной на соискание ученой степени кандидата технических наук по специальности 2.2.15 – Системы, сети и устройства телекоммуникаций.

С развитием и усложнением средств, методов и форм автоматизации процессов обработки и передачи информации в телекоммуникационных сетях централизованной охраны объектов (ТКС ЦОО), наблюдается увеличение уязвимости системных процессов и ресурсов. Данный аспект напрямую влияет на возможность уничтожения, блокирования или искажения информации о состоянии централизованно охраняемых объектов, а также приводит к появлению "нештатных" процессов, что создает ситуацию, когда основные функции системы теряют свою эффективность.

Снижение работоспособности ТКС ЦОО обусловлено различными факторами, такими как просчеты в формировании инфраструктуры компонентов ТКС ЦОО, ошибки в реализации программных и аппаратных компонентов, преднамеренные информационные воздействия, ошибки операторов и старение оборудования. Для обеспечения стабильной работоспособности ТКС ЦОО необходимо иметь возможность прогнозирования всех возможных угроз вторжения, а также выхода из строя компонентов системы. Это позволит повысить уровень защищенности структурных компонентов ТКС ЦОО и устранить уязвимости.

Для текущей оценки и прогнозирования работоспособности ТКС ЦОО требуются средства моделирования оценки информационной защищенности компонентов с учетом прогнозируемых угроз. На данный момент существующие модели функционирования ТКС ЦОО не обладают такой возможностью.

Задачами, решаемыми в диссертационной работе, являются:

- построение модели работоспособности ТКС ЦОО, позволяющую анализировать работу телекоммуникационной сети в условиях действия дестабилизирующих воздействий;

- разработка средств моделирования процессов обеспечения информационной безопасности в ТКС ЦОО, включая базы данных угроз, уязвимостей компонентов ТКС ЦОО, защитных механизмов, модель нарушителя информационной безопасности;

- разработка алгоритмов определения степени проявления уязвимости и силы защитных механизмов ТКС ЦОО;

- разработка методики проведения аудита работоспособности ТКС ЦОО и показать ее адекватность на практике.

В ходе проведения исследований по теме диссертационной работы автором получен ряд результатов, обладающих научной новизной, практической значимостью и выдвигаемых на защиту:

1. Предложена модель работоспособности ТКС ЦОО, определяемая функцией вероятностей защищенности компонентов телекоммуникационной сети на основе анализа ее инфраструктуры и условий эксплуатации.

2. Разработаны алгоритмы:

- оценки вероятности реализации угрозы при наличии уязвимости компонента ТКС ЦОО, отличающийся вновь выявленными закономерностями между типом угроз и способами проявления уязвимостей;

- оценки вероятности опасности угроз в компонентах ТКС ЦОО с учетом защитных механизмов, отличающийся вновь выявленными закономерностями между типом угроз, способом и характером действия защитных механизмов;

- определения степени проявления уязвимостей и силы защитных механизмов, выявляемых в компонентах ТКС ЦОО, оригинальность которого основана на их декомпозиции в зависимости от условий эксплуатации компонентов.

3. Усовершенствована модель оценки вероятности информационной защищенности компонента ТКС ЦОО, оригинальность которой состоит в том, что в модель включен элемент «Нарушитель» и сопутствующие ему параметры.

Основные результаты работы являются достоверными, что обусловлено корректностью постановки задач исследования, подтверждается корректным использованием математических методов, результатами вычислительных экспериментов, а также проведением пробных расчетов работоспособности ТКС ЦОО.

Полученные в диссертации результаты в целом развивают методологию обеспечения конфиденциальности, целостности и доступности в телекоммуникационных сетях централизованной охраны объектов. Содержание основных положений и результаты диссертации докладывались на международных и всероссийских научно-технических конференциях.

Практическая значимость работы заключается в том, что предложенные в данной работе модели и алгоритмы позволяют проводить оценку защищенности информационных процессов по показателям конфиденциальности, доступности и целостности, и прогнозировать изменения состояния работоспособности структурных компонентов ТКС ЦОО для всех режимов функционирования, что позволяет выборочно применять защитные механизмы, усиливающие защищенность элементов системы.

Разработанное программное обеспечение позволяет рассчитывать вероятности опасности угроз по последствиям их реализации с учетом защитных механизмов (свидетельство о государственной регистрации программы для ЭВМ №2022682661), вероятности реализации угрозы (свидетельство о государственной регистрации программы для ЭВМ №2022680341).

Замечание и недостатки:

1. В заключении к работе (стр. 136) не указано про уровень ложных срабатываний, о чем было сказано в предыдущих выводах, и неясно, какое количество ложных срабатываний бралось за эталонное, исходя из практики функционирования ПЦО в ТКС ЦОО.

2. Из представленного в работе Входе проведения пробного расчета показателей работоспособности структурных компонентов ТКС ЦОО для 25 охраняемых объектов разных категорий неясно, сколько и каких охранных извещателей находилось на каждом объекте.

3. Не ясно, каким образом можно проверить на практике снижение количества ложных срабатываний на ПЦО при практическом использовании результатов оценки работоспособности структурных компонентов ТКС ЦОО.

4. В тексте диссертационной работы присутствуют опечатки

Однако, отмеченные недостатки не носят принципиального характера и не наносят существенного ущерба значимости результатам диссертационной работы, выполненной на высоком научном уровне. Отличительными особенностями работы являются логическая последовательность поставленных задач и направленность на решение важной практической технической задачи, а именно оценки работоспособности телекоммуникационной сети централизованной охраны объектов.

Основные выводы и положения диссертации апробированы в научных изданиях и докладывались на научно-технических конференциях различного уровня. Требование ВАК о наличии публикаций в изданиях из перечня ВАК выполнено.

Содержание автореферата соответствует основным положениям диссертации и позволяет сформировать обоснованное представление по всей работе в целом, а содержание диссертации соответствует паспорту специальности 2.2.15 – Системы, сети и устройства телекоммуникаций, конкретно пунктам 17, 19.

