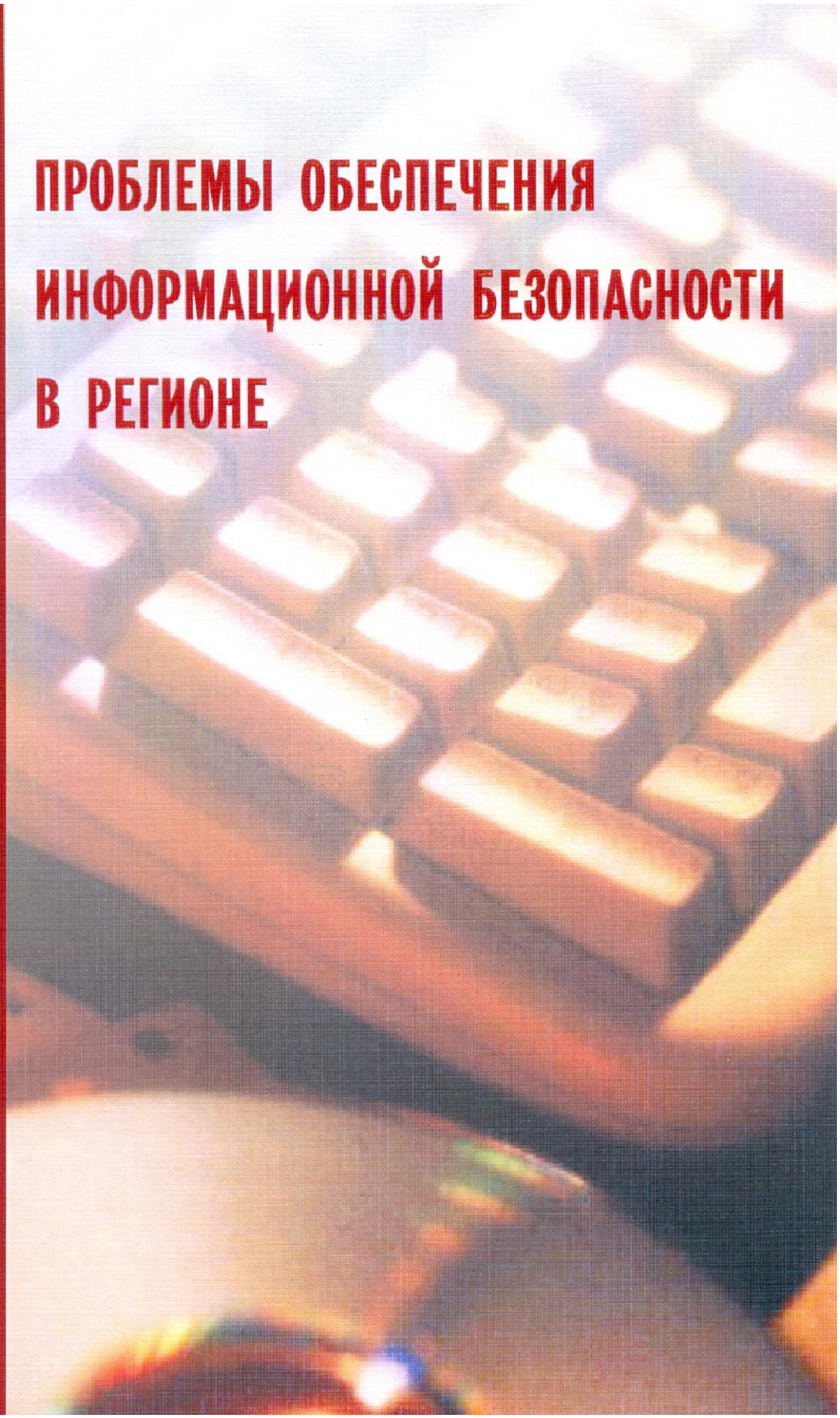
ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕГИОНЕ

Материалы региональной научно-практической конференции г. Волгоград, 28 марта 2008 г.



УДК 004
ББК 32.81

Проблемы обеспечения информационной безопасности в регионе: Сборник трудов региональной научно-практической конференции / Волгоград, 28 марта 2008 года. – В.: Волгоградский государственный университет, 2008. – 106 с.

Сборник содержит доклады и тезисы, представленные на региональную научно-практическую конференцию «Проблемы обеспечения информационной безопасности в регионе», проведенную 28 марта 2008 года в Волгоградском государственном университете.

Основные секционные направления работы конференции: проблемы информационной безопасности в корпоративных сетях государственных учреждений г. Волгограда; проблемы сертификации объектов информатизации в г. Волгограде.

ПОСТРОЕНИЕ МОДЕЛИ СИСТЕМЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ

А. В. Никишова

Волгоградский государственный университет

Наблюдающийся в последние годы процесс бурного развития компьютерных сетей, информационных технологий, а так же глобального информационного обмена поставил ряд серьезных вопросов, связанных с защитой информации.

Процесс управления защитой информации состоит из следующих этапов:

1. Организация сбора данных о состоянии системы защиты и воздействии дестабилизирующих факторов, приводящих к утечке информации;
2. Анализ данных и оценка уровня безопасности информации на объекте ее обработки;
3. Определение способа достижения требуемого уровня и выработка управленческие решения по использованию необходимых методов и средств защиты информации;
4. Анализ качества принятых мер, т.е. оценка эффективности их применения.

Возросшая сложность компьютерных сетей и механизмов защиты, увеличение количества уязвимостей и потенциальных ошибок в их использовании, а также возможностей по реализации атак обуславливают трудности ручного сбора данных о состоянии защищенности системы. Поэтому существует необходимость использования автоматизированных средств сбора данных о состоянии защищенности системы – сканеров уязвимостей. Однако информация, которую выдает сканер уязвимостей, отражает только лишь обнаруженные им уязвимости. Он не способен выявить то, как уязвимости могут взаимодействовать между собой в информационной системе. К примеру, сканер не может отследить, как нарушение безопасности на одной из машин может повлиять на защищенность других машин в системе. Однако эта ситуация может быть выявлена на этапе анализа данных.

Анализ собранных данных весьма сложная задача, и ее полная автоматизация практически невозможна. Однако использование графов атак может облегчить процесс анализа собранных данных и оценки безопасности информации на объекте ее обработки. Графы атак являются методом, с помощью которого можно обнаруживать и исследовать взаимодействие между уязвимостями всей системы. При построении графа атак используется информация о различных типах атакующих действий, учитывается первоначальное положение нарушителя, конфигурация компьютерной сети и реализуемая в ней политика безопасности. Вершины графа представляют хосты и атакующие действия. Дуга соединяет вершины в случае возможности осуществления атакующего действия нарушителем. При формировании графа атак необходимо реализовать действия по перемещению нарушителя с одного хоста на другой и атакующие действия, использующие уязвимости программного и аппаратного обеспечения. Таким образом, граф атак может выявлять, на основе топологии сети, все возможные пути достижения цели злоумышленником, учитывая влияние реализации одной из угроз на реализуемость других угроз.

Следующим шагом управления является выявление из всех возможных путей достижения цели злоумышленником наиболее вероятного пути его проникновения, что поможет определить первоочередные направления усиления системы защиты, наиболее необходимые методы и средства защиты информации. Этот анализ может не только определить перечень мер, позволяющих предотвратить использование уязвимостей, но также и наименьшее множество мер, реализация которых сделает сеть защищенной. Это позволит сделать систему защиты более эффективной, затрачивая при этом меньшие (в первую очередь экономические) средства.

Для анализа качества принятых мер необходимо периодически проводить аналогичный анализ для вновь собираемых данных о состоянии защищенности системы. Однако из-за большой трудоемкости данного процесса целесообразно применение систем диагностики атак. Эти системы помогут обнаружить возникновение атаки, что является свидетельством наличия каких-то вновь обна-

руженных уязвимостей. Что может свидетельствовать о том, что анализ уязвимостей необходимо провести снова, и вновь выработать решения для усиления системы защиты.

Таким образом, основной задачей систем диагностики атак должно стать обнаружение новых атак и типов атак. Это может быть достигнуто применением систем диагностики атак, использующих для анализа нейронные сети. Адаптивность нейронных сетей может позволить выявить новые атаки. Кроме этого необходимо проводить как можно более полный мониторинг. А потому наиболее подходящими являются системы диагностики атак, проводящие мониторинг как на системном так и на сетевом уровнях. Данная система диагностики атак собирает данные о происходящих в операционной системе каждой машины событиях и передаваемых в системе пакетах и проводит анализ собранных данных с помощью обученных для этого нейронных сетей. Обнаружение данной системой отклонений от нормальной работы становится сигналом о возможных действиях, направленных на нарушение защищенности системы.

Список литературы

1. Колегов Д.Н. Проблемы синтеза и анализа графов атак. г. Томск, 2007
2. Степашкин М.В., Котенко И.В., Богданов В.С. Интеллектуальная система анализа защищенности компьютерных сетей. СПб., 2006
3. Danforth M. Models for threat assessment in networks. 2006

ПРОБЛЕМА СЕРТИФИКАЦИИ ПРОГРАММ ДЛЯ ГЕНЕРАЦИИ ТЕСТОВОГО СИГНАЛА ПРИ ПРОВЕДЕНИИ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

М. А. Кирпо

ФГУП "ЦКБ "Титан"

При проведении аттестации объектов информатизации одним из составляющих элементов является проведение специальных исследований средств