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

УДК 004.056

Лось
Павел Николаевич

Методы и средства комплексного анализа информационной безопасности компьютерных систем

АВТОРЕФЕРАТ

на соискание степени магистра технических наук по специальности 1-31 80 10 «Теоретические основы информатики»

Научный руководитель
В. В. Захаров
кандидат технических наук,
доцент кафедры ИИТ

Минск 2020

ВВЕДЕНИЕ

Быстрое совершенствование цифровых технологий и использования цифровых устройств в качестве хранилища информационных ресурсов привели к тому, что вопрос защиты цифровых и компьютерных устройств стоит как никогда остро.

Защитить компьютеры от атаки очень сложно. Защита должна содержать широкий спектр модулей, включая традиционный антивирус, персональный файервол, веб-фильтрацию и защиту почты, контроль устройств. Традиционные решения защиты эффективны при блокировке известных угроз. Однако они не способны защитить от угроз, которые используют «окно возможностей» — время между появлением нового вируса и выпуском противоядия антивирусными компаниями. Увеличивающийся разрыв используется хакерами для распространения вирусов, «шифровальщиков», троянов и других типов угроз.

Кроме того, в последнее время мы все чаще слышим о «постоянных угрозах повышенной сложности» (APT). Такие угрозы предпочитают скрытно проникать в ИТ-систему предприятия и, находясь там на протяжении нескольких месяцев и даже лет, осуществлять свои вредоносные действия: как правило, это кража конфиденциальной информации. Возникает тревожная ситуация, когда предприятие, уверенное в эффективности и надежности своей защиты, даже не подозревает о наличии серьезных проблем.

Мишенью могут стать любые предприятия: не только крупные, но и небольшие. Зачастую злоумышленникам проще поразить сотни мелких компаний и с каждого из них потребовать соответствующий выкуп за конфиденциальную или персональную информацию.

Несмотря на то, что в организациях используется множество инструментов для противодействия угрозам, информация, раскрываемая этими инструментами безопасности, в основном представляет собой очень плохоструктурированное исследование текущего состояние системы. Вот почему организации нанимают специалистов, чтобы обработать все собранные данные и проанализировать любые возможные уязвимости. Обычно они заканчиваются графиком того, как существующие уязвимости в системе могут привести к одной или нескольким потенциальным атакам. Таким образом, существует острая необходимость в более глубоком понимании отчетов безопасности, чтобы полностью понять, что на самом деле происходит в системе.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность

Информация является ценным ресурсом, и повреждение целостности (неизменности), конфиденциальности или доступности которого может привести к серьезным последствиям, таким как снижение конкурентоспособности на рынке и экономическим потерям. В результате большинство компаний стремятся внедрить различные системы безопасности, чтобы защитить этот ресурс. Однако определить качество внедренных механизмов защиты является сложной и нетривиальной задачей. Зачастую для решения данной проблемы, организациям необходимо прибегать к помощи высококвалифицированных экспертов в области ИБ, как правило, нанимаемых со стороны. Вытекающими недостатками этого является высокая стоимость, а также потраченное время для поиска специалистов, которые способны произвести анализ систем безопасности. Возможное решение этих проблем, является разработка автоматизированной системы для анализа защиты информации, которая поможет повысить оперативность процесса анализа, а также снизить финансовые расходы.

Цель и задачи исследования

Целью исследования является снижение трудозатрат анализа ИБ и повышение уровня защищенности компьютерных систем.

Задачи исследования:

– исследовать проблемы ИБ;

– проанализировать существующие подходы к анализу ИБ;

– разработать методику обеспечения ИБ;

– разработать концепцию и средства для анализа безопасности ИБ.

Объект исследования: процесс проведения комплексного анализа информационной безопасности компьютерных систем

Предмет исследования: методы и средства комплексного анализа информационной безопасности компьютерных систем.

Структура и объем диссертации

Диссертация состоит из перечня условных обозначений, введения, трёх глав, заключения, списка использованных источников.

В первой главе представлен анализ предметной области – проблемы обеспечения ИБ и рассмотрены существующие средства и методы анализа ИБ. Рассмотрены средства анализа защищенности операционных систем, сетевых протоколов и сервисов. Выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения. Выявлены требования к системам анализа информационной безопасности. Вторая глава посвящена разработке метода анализа ИБ с помощью экспертных систем. В третьей главе была детально рассмотрена архитектура разрабатываемой системы. Были описаны входные и выходные данные, рассмотрены основные модули системы и их функции. Заключение включает основные выводы по работе.

Общий объем работы составляет 62 страницы, 20 рисунков на 10 страницах и списка использованных источников из 26 наименований на 2 страницах.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В диссертации исследуются методы и средства для анализ информационной безопасности компьютерных систем. Выявлены требования для систем анализа ИБ. Рассмотрены существующие методы и средства анализа ИБ. Исследованы практические варианты построения сиситем анализа на основе экспертных систем.

В первой главе представлен анализ предметной области – проблемы обеспечения ИБ и рассмотрены существующие средства и методы анализа ИБ. Рассмотрены средства анализа защищенности операционных систем, сетевых протоколов и сервисов. Рассмотрены методы обеспечения анализа: статистический метод, экспертные системы, нейронные сети. Выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения. Выявлены требования к системам анализа информационной безопасности.

Вторая глава посвящена разработке метода анализа ИБ с помощью экспертных систем. В данном разделе рассмотрены принципы построения экспертной системы. Были выбраны модель представления знаний, способ ввода знаний и основные источники для использования базы знаний.

В третьей главе детально рассмотрена архитектура разрабатываемой системы. Описаны входные и выходные данные, рассмотрены основные модули системы и их функции. Дана характеристика пользователей системы, их функции и возможные сценарии работы пользователей с системой. Определена модель данных для функционирования системы и приведены пример правил, на основе которых производится анализ безопасности.

Заключение включает основные выводы по работе.

ЗАКЛЮЧЕНИЕ

В результате выполнения диссертационной работе бала спроектирована система для анализа информационной безопасности компьютерных систем на основе экспертной системы. Применение ЭС для обеспечения информационной безопасности позволяет существенно повысить уровень информационной безопасности, упростить процесс обнаружения и анализа проблем информационной защиты, а так же использовать опыт экспертов в области информационной безопасности.

В рамках диссертации рассмотрены и решены следующие задачи:

– проведен анализ существующих подходов к построению систем анализа ИБ, проведен обзор систем для анализа потенциальных угроз как на уровне операционной системы, так и на уровне сетевых протоколов, рассмотрены технологии и средства разработки таких приложений, выделены требования к разрабатываемой системе;

– на основе результатов анализа и требований выбраны методы для построения экспертной системы анализа защищенности, описана модель представления знаний, подсистема вывода и алгоритм поиска по базе знаний, рассмотрены источники знаний для системы анализ ИБ;

– сформулированы задачи, которые должны решаться в системе анализа ИБ, описано взаимодействие между пользователями, спроектирована архитектура приложения, выделены его основные подсистемы и модули, спроектирована модель данных и рассмотрен процесс создания правил для ЭС;

Характерными особенностями разработанного веб-приложения являются:

– многоуровневая архитектура;

– помощь в выявлении потенциальных опасных ситуаций;

– четкая спецификации логики рассуждений;

– легкость внесения дополнений и изменений в систему правил

Дальнейшее возможное развития, это расширение системы с помощью других методов искусственного интеллекта, например нейронных сетей для динамического выявления совершенно новых, неописанных ранее атак и уязвимостей.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Лось П.Н. Использование экспертных систем для анализа и оценки информационной безопасности / Лось П.Н. // 56-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» – Минск, 21–24 апреля 2020 – С.15

2. Лось П.Н. Построение модели базы знаний для экспертной системы аудита безопасности / Лось П.Н. // 56-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» – Минск, 21–24 апреля 2020 – С.16