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

УДК 004.732:004.056

Книга
Николай Михайлович

Методика обнаружения уязвимостей в корпоративной сети предприятия

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты, информационная безопасность

_____

Научный руководитель
Ширинский Валерий Павлович
кандидат технических наук, доцент

_____

Минск 2016

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время существует множество корпоративных сетей со сложной структурой, большим числом элементов и информационных связей, чаще всего находящихся в общем информационном пространстве. Из-за подверженности ИС внутренним и внешним угрозам, несовершенству их реализации, а также высокой стоимости хранящейся и обрабатываемой в них информации возникает задача обеспечения информационной безопасности ИС. Она осложняется тем, что устранение большинства угроз ИС требует усовершенствования их отдельных элементов, что не всегда возможно ввиду их закрытости и сложности (операционная система, драйверы, программное обеспечение сторонних обработчиков).

Так как не всегда возможны изменение или замена одних элементов ИС на другие в силу различных причин и ограничений, то для решения задачи обеспечения информационной безопасности ИС необходимо внесение изменений в структуру ИС. Это можно сделать путем добавления новых элементов, удаления или замены старых на более надежные и безопасные, если такое возможно, и изменения информационных связей между элементами ИС. Основной задачей таких изменений будет устранение или минимизация влияния внутренних и внешних угроз информационной безопасности ИС, вносимых всеми ее элементами.

Решить задачу обеспечения информационной безопасности ИС позволяет аудит информационной безопасности КСП. Однако отсутствует (не закрепленность в ТНПА) в Республике Беларусь в настоящее время единой специализированной методика оценки уязвимостей в КС не позволяет разрабатывать эффективные методы обнаружения большинства видов несанкционированных действий и атак в сети ИС. Этим объясняется актуальность исследования в этой области.

Попыткой систематизации знаний в области обнаружения сетевых атак являются работы Лукацкого А.В., обобщенные в книге «Обнаружение атак». Согласно которой большинство существующих методов основано на личных предпочтениях аудитора. Анализ принципов работы современных СОА подтверждает эти выводы. Несмотря на возрастающую с каждым днем сложность политики безопасности ИС, в современных методах обнаружения уязвимостей практически не учитывается проблема обнаружения несанкционированных действий в сети.

Для оценки ИБ сети не всегда можно найти эталонную методику и необходимо учитывать особенности ее функционирования, то становится актуальной задача разработки типовой методики оценки ИБ сети.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 5.5 «Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2011 – 2015 гг., утверждённых Постановлением Совета Министров Республики Беларусь 19 апреля 2010г., № 585. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке общей методике обнаружения уязвимостей в корпоративной сети предприятия.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать современные стандарты и методики в области анализа защищенности сети.
2. Разработать типовую методику аудита корпоративной сети предприятия.
3. Провести апробацию предложенной методики.

Личный вклад соискателя

Все основные результаты, выводы получены соискателем самостоятельно. Методика обнаружения уязвимости в корпоративной сети предприятия также разработана самостоятельно.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на 51-й научной конференции аспирантов, магистрантов и студентов (Минск 2015) и XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, 2015).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 работа, в том числе 1 статьи в сборниках материалов конференций.

КРАТКОЕ СОДЕРЖАНИЕ

Работа состоит из введения, трех глав и заключения.

В первой главе “Средства анализа защищенности” рассмотрены основные методы обнаружения атак в сетях, выделены их достоинства и недостатки.

Рассмотрены наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности компьютерной сети:

- ISO 15408: Common Criteria for Information Technology Security Evaluation.

- Code of practice for Information Security Management/ISO 17799.

Также проанализированы нормативные документы в Республике Беларусь в области обеспечения безопасности информационных систем, в частности компьютерных сетей.

Во второй главе «Корпоративная сеть предприятия» рассмотрен объект исследования – корпоративная сеть. Проанализированы их достоинства и возможности по организации различных видов услуг и сервисов.

Приведены различные классификации уязвимостей в корпоративной сети, также рассмотрены угрозы: конфиденциальности, целостности, доступности, аутентичности, наблюдаемости.

В третьей главе “Методика обнаружения уязвимости в корпоративной сети предприятия” исследованы методики защиты корпоративной сети от различных угроз.

Рассмотрены методы тестирования корпоративной сети.

Представлена типовая методика обнаружения уязвимостей в корпоративной сети предприятия. Описаны исходные данные, которые должен представить заказчик при проведении работ по аттестации безопасности его корпоративной сети.

ЗАКЛЮЧЕНИЕ

В настоящее время в Республике Беларусь отсутствует (не закреплена в ТНПА) единая специализированная методика оценки уязвимостей в компьютерной сети. Также отсутствует общая методология построения систем обнаружения уязвимостей, поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться.

В магистерской работе были проанализированы существующие угрозы и уязвимости ИС и методы защиты от них, и представлена типовая методика обнаружения уязвимости в КСП. Она состоит из пяти шагов:

– Изучение исходных данных компьютерной сети и анализ состава, структуры и конфигурации критических элементов сетевой инфраструктуры;

– Сканирование внешних сетевых адресов компьютерной сети из сети Интернет;

– Сканирование ресурсов компьютерной сети изнутри;

– Анализ конфигурации компьютерной сети, серверов и рабочих станций сети при помощи специализированных средств контроля защищенности;

– Обработка полученных результатов тестирования.

Эта методика предполагает применение как активного, так и пассивного тестирования системы защиты. Активное тестирование заключается в эмуляции действий потенциального злоумышленника; пассивное тестирование предполагает анализ конфигурации операционной системы и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную или с использованием специализированных программных средств.

При проведение аудита корпоративной сети предприятия особое внимание следует уделять внутренним утечкам информации, которые, за первое полугодие 2015, составили 65% от общего количества утечек.

В рамках магистерской работы также представлен перечень исходных данных и документации необходимой для аудитора корпоративной сети предприятия, использующего данную методику.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Н.М. Книга, В.П. Ширинский. Аудит корпоративной сети предприятия. // Технические средства защиты информации: тезисы докладов XII Белорусско-российской науч.-техн. конф. – Минск: БГУИР,2015 – С.9.