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

УДК 621.398

Цымбалов
Алексей Дмитриевич

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННОЙ СЕТИ

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-39 80 01 «Радиосистемы и радиотехнологии»

_____

Научный руководитель
Гринкевич Антон Витальевич
кандидат технических наук, доцент

_____

Минск 2021

Краткое введение

В настоящее время в мире функционирует более 3,5 миллионов электронно-вычислительных машин и 12000 локальных вычислительных сетей, 95% военных линий связи проходят по телефонным каналам связи общего пользования. По итогам 2018 года в США зафиксировано 450000 случаев попыток вторжения в информационно-вычислительные системы государства, 260000 в системы различных министерств, при этом 292500 (65%) были удачными. Именно поэтому вопросы безопасности информации на современном этапе рассматриваются как приоритетные в государственных структурах, научных учреждениях, коммерческих организациях. Информационные системы специального назначения (банковские системы, системы силовых ведомств и т.п.), являясь приоритетным в структуре государства, не могут оставаться в вопросах обеспечения информационной безопасности на уровне традиционных средств защиты информации (криптографической защиты, разграничения доступа и т.д.).

Существующие на сегодняшний день методы и средства защиты информации в информационно-вычислительных системах достаточно разнородны из-за разнообразных способов и средств несанкционированных действий. Главным недостатком существующих методов и средств защиты информации, включая современные средства поиска уязвимостей автоматизированных систем и обнаружения несанкционированных действий, является то, что они, в большинстве случаев организуют защиту информации лишь от уже выявленных угроз, что показывает определенную степень пассивности защиты.

Адекватный уровень защиты информации можно обеспечить применением комплексного подхода предполагающего использование традиционных организационных и программно-технических средств.

Одним из возможных направлений решения проблемы защиты информации в локальной информационной сети от несанкционированных действий, является применение методов обмана. Такие системы получили название ложных или обманных.

Механизм функционирования обманной системы заключается в том, чтобы вовлечь злоумышленника (злоумышленник или легальный пользователь, нарушающий политику безопасности) в диалог с системой. При этом обманные системы имитируют уязвимости реальных информационных систем. Злоумышленнику приходится постоянно решать: работает он с реальной системой или обманной, затрачивая при этом ресурсы (время, вычислительные мощности и т.п.).

Таким образом, использование обманных систем защиты информации в качестве защитного (маскировочного, дезинформирующего) механизма повышает шансы администратора сети вычислить нарушителя, блокировать его незаконные действия или осуществить корректировку политики безопасности.

В данных материалах приведено описание работы типовой обманной системы защиты информации и выбраны показатели качества ее функционирования. На основе анализа литературы была составлена подробная классификация методов обмана, применяющихся в обманной системе защиты информации, и определено место ОБС в общей классификации систем защиты информации.

Общая характеристика работы

Цели и задачи исследования:

Повышение защищенности информации в локальной информационной сети с системой обмана.

Научная проблема (задача):

Определение показателя и оценка эффективности защиты информации в локальной информационной сети с системой обмана.

Практические задачи:

1. Выбрать показатель эффективности защиты информации в локальной информационной сети с системой обмана.
2. Провести оценку выбранного показателя эффективности защиты информации в локальной информационной сети с системой обмана.
3. Выработать рекомендации по повышению эффективности защиты информации в локальной информационной сети с использованием обманной системы.

Объект исследования: локальная информационная сеть с системой обмана.

Предмет исследования: эффективность защиты информации в локальной информационной сети с системой обмана.

Выбор объекта исследования обусловлен необходимостью определить влияние применения обманной системы защиты информации на вероятность несанкционированного доступа к ресурсам локальной информационной сети.

Положения, выносимые на защиту:

1. Рекомендации по повышению эффективности защиты информации в локальной информационной сети с использованием обманной системы.
2. Результаты аналитических и экспериментальных исследований оценки эффективности защиты информации в локальной информационной сети с системой обмана.

Личный вклад соискателя:

Представленные в диссертационной работе основные теоретические и практические результаты, а также положения, выносимые на защиту, получены соискателем самостоятельно и в полной мере отражены в опубликованных печатных работах. Научному руководителю в совместных работах принадлежат предметные постановки задач, выбор направлений исследований, обсуждение результатов. В публикациях с соавторами вклад автора определяется рамками излагаемых в диссертации результатов.

Апробация результатов диссертации

Результаты исследований докладывались на следующей конференции:

1. Республиканская научно-техническая конференция «Информационные радиосистемы и радиотехнологии 2020».

Опубликованность результатов диссертации

По теме диссертации опубликована 1 печатная работа в сборнике трудов и материалов конференций в БГУИР.

Структура и объем диссертации

Диссертация состоит из общей характеристики работы, введения, трех глав, заключения, библиографического списка и одного приложения.

В первой главе приведен анализ способов (методов) несанкционированных действий на локальную информационную сеть.

Во второй главе приводится анализ механизма функционирования обманных систем защиты информации в локальной информационной сети.

В третьей главе приводятся результаты исследований по оценке эффективности применения обманных систем защиты информации в локальной информационной сети, даются рекомендации по применению в локальных информационных сетях.

Общий объем работы составляет 64 страницы, из которых основного текста – 57 страниц, 17 рисунков, 10 таблиц, список использованных источников из 20 наименований на 2 страницах.

Основное содержание

Во **введении** определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика вопроса.

Первый раздел «Анализ способов (методов) несанкционированных действия на локальную информационную сеть» носит теоретический характер. В данном разделе приведен анализ способов (методов) несанкционированных действий на локальную информационную сеть, рассмотрено понятие информационной сети, приведена структура информационного противостояния.

Во **втором разделе** «Анализ систем обмана» приводится описание механизма функционирования обманных систем в системе защиты информации в локальной информационной сети. Определены показатели эффективности защиты информации в локальной информационной сети с системой обмана.

Третий раздел «Оценка эффективности применения обманных систем защиты информации в локальной информационной сети» посвящен выбору приоритетных показателей эффективности применения обманных систем защиты информации в локальной информационной сети, оценке приоритетных показателей эффективности применения обманных систем защиты информации в локальной информационной сети, разработке рекомендаций по повышению защищенности локальной информационной сети с системой обмана.

Заключение

В ходе диссертационных исследований проанализированы отечественные и зарубежные источники, посвященные построению и применению обманных систем защиты информации, а также оценки эффективности их применения в локальных информационных сетях. Результаты анализа позволили составить описание работы типовой обманной системы защиты информации и выбрать показатели качества ее функционирования. На основе анализа литературы составлена подробная классификация методов обмана, применяющихся в обманной системе защиты информации, и определено место ОБС в общей классификации систем защиты информации. В результате этого анализа определено, что для проведения обмана противника существуют три общих варианта обмана: сокрытие, камуфляж и дезинформация. В зависимости от строения локальной информационной сети и преследуемых целей различают два основных варианта размещения обманной системы защиты информации в локальной информационной сети. Каждый вариант размещения описан графически на основе анализа применения ОБС в реальных ЛИС. Также в диссертационной работе на основе анализа литературы по оценке эффективности применения ОБС определены основные подходы к оценке эффективности ОБС. В работе приведено математическое моделирование функционирования ОБС в момент информационной атаки на ЛИС. Для определения влияния количества эмулируемых ОБС ложных объектов на вероятность несанкционированного доступа к целевым объектам проведен эксперимент на реально функционирующей ЛИС. Анализ результатов эксперимента показал, что применения ОБС может значительно снизить вероятность несанкционированного доступа к целевым объектам, вплоть до полной неспособности противника осуществить НСД к целевым объектам ЛИС. На основании анализа литературы и результатов математического моделирования и эксперимента выработаны рекомендации по повышению защищенности ЛИС и оценки эффективности применения ОБС, учитывающего как возможности распознавания ложных и истинных объектов, так и динамику функционирования самой защищаемой ЛИС.

Список опубликованных работ

1. Цымбалов А.Д., Гринкевич А. В. Проведение информационной атаки на локальную информационную сеть // Республиканская научно-техническая конференция «Информационные радиосистемы и радиотехнологии 2020» (Республика Беларусь, г.Минск, 28-29 октябрь 2020). – Минск: БГУИР, 2020.