ВВЕДЕНИЕ

Актуальность исследования.

В настоящее время все более актуальной становится задача защитыинформационных ресурсов компьютерных сетей от атак со стороны внешних ивнутренних нарушителей. Методика взлома компьютерных сетей совершенствуется практически с той же скоростью, с которой создаются средства защиты информации, наиболее популярными из которых являются: межсетевое экранирование, разграничение доступа, шифрование, идентификация и аутентификация. Новые технологии и программные продукты останавливают злоумышленников лишь на время, так как имеют один существенный недостаток: все они схожи со своими предшественниками по принципу работы: общие алгоритмы мало чем отличаются друг от друга у различных производителей, новые функциональные особенности содержат ошибки и т.п. Все это только на время останавливаетнарушителя, заставляя искать очередную уязвимость в продукте, зачастую унаследованную от прошлых версий. Ярким примером вышесказанному могут послужить частые случаи взлома компьютерных сетей крупных международных компаний, нарушение правильной работы фондовых бирж, утечка служебной информации из различных государственных структур [1-3].

Применительно к противодействию информационно-технологическим атакам на информационные ресурсы АС необходимо отметить, что в настоящее время разработаны методы противодействия указанным угрозам, которые, однако, носят пассивный характер (прекращение передачи информации, закрытие канала связи, изменение маршрутизации и т.п.), что предоставляет злоумышленнику информацию о том, что его воздействие обнаружено, и оставляет в его руках инициативу выбора места, времени и способа повторных атак.

Современные автоматизированные системы носят распределенный характер, из-за чего невозможно гарантировать абсолютную защиту от НСД. Вследствие этого для повышения эффективности защиты информации требуется создание и использование принципиально новых, специфических средств скрытого активного

противодействия вторжениям в автоматизированную систему. В настоящее время ведутся работы по созданию подобных механизмов защиты, одним из которых является ложная информационная система [7,8,11,14,24,28].

Главный отличием данного средства защиты от других является сокрытие его присутствия в системе и направленность на обман злоумышленника, в отличие от классического блокирования доступа, свойственного другим средствам защиты. Это позволяет не только защитить хранимую в компьютерных сетях информацию, но и проанализировать действия злоумышленника, используя полученные сведения для дальнейшего совершенствования системы защиты информации. В этом заключается особенность данного средства защиты – расчет не только на программно-аппаратный набор компонентов системы защиты и использование технических методов и средств, но и «игра в прятки» со злоумышленником в попытке заманить его на данную ложную систему [17-19, 32-36].

Принцип работы ложной информационной системы довольно простой – любому субъекту, желающему получить доступ к объекту, предлагается пройти процедуру идентификации (к примеру, ввести пароль). Если проверка проходит успешно, то субъект получает доступ. Если проверка прошла неудачно или у системы безопасности «возникли подозрения», то субъект автоматически переводиться на ложную систему, которая в достаточной степени эмулирует объект. Таким образом, если субъект пытался получить незаконный доступ к объекту, то для него создается впечатление, что попытка взлома прошла успешно [43-45].

Ложные информационные системы позволяют в режиме реального времени выявлять атаки и направлять их по ложному следу. То есть злоумышленник тратит на ловушки и ложные целивремя, которое администраторы безопасности могут использовать для сбора необходимых сведений об атаках или для идентификации злоумышленника. Благодаря использованию ЛИС сокращаются издержки на администрирование системы, в результате защита становится более гибкой и эффективной.

Цель и задачи исследования.Целью настоящей работы являетсяразработка требований и путей построения перспективной ложной информационной системы, в интересах защиты компьютерных сетей от удаленных атак, а также разработка подхода для оценки эффективности от ее применения.

Для достижения поставленной цели в работе решались задачи:

1. исследование основных особенностей примененияложных информационных систем,как средства защиты от НСД к информации, обрабатываемой в КС;
2. создание вербальной модели ложной информационной системы, как средства защиты от НСД к информации, обрабатываемой в КС;
3. оценка результатов применения ложных информационных систем, как средства защиты от НСД к информации, обрабатываемой в КС, для различных типов атак;
4. практическая оценка эффективности применения ЛИС, как средства управления рисками в интересах защиты от НСД информации, обрабатываемой в КС;
5. оценка экономических показателей ложной информационной системы, как средства защиты от НСД к информации, обрабатываемой в КС;

Объект исследования. Объектом исследования является ложная информационная система, как средство защиты от НСД к информации, обрабатываемой в КС.

Предмет исследования. Предметом исследования является оценка эффективности применения ложных информационных систем, как средства защиты от НСД к информации, обрабатываемой в КС.

Методы исследования.Для реализации намеченной цели исследования и решения поставленных задач используются методы построения систем защиты информации, теории рисков, теории вероятности, математической статистики и системного анализа, теории информации,методы имитационного моделирования.

ЗАКЛЮЧЕНИЕ

Работа посвящена исследованию возможности управления рисками автоматизированных систем на основе использования ложных информационных систем.В ходе еѐ выполнения были получены следующие основные результаты:

1. Проведено исследование основных особенностей применения ЛИС, как средства защиты от НСД к информации, обрабатываемой в КС. Приведено описание ЛИС, выявлены достоинства и недостатки их применения для защиты КС от удаленных атак. Проведена классификация ЛИС по различным признакам, описаны входящие в них компоненты.

2. Построена вербальная модель ЛИС,как средства защиты от НСД к информации, обрабатываемой в КС. Проанализированы и разработаны основные требования, предъявляемые к функциональным возможностям и архитектуре ЛИС и ее компонентов, после чего проведено моделирование ее архитектуры.

3. Проведена оценка результатов применения ложных информационных систем, как средства защиты от НСД к информации, обрабатываемой в КС, для различных типов атак. Разработан подход для оценки степени подобия ЛИС целевой системе, основанный на методе экспертных оценок. Описана динамика возникновения угроз связанных с несанкционированным доступом к информации в компьютерной сети, с использованием аппарата марковских процессов, в результате чего построена марковская модель для некоторых типов сетевых атак.

4. Выбран способ реализации ЛИС. Описаны основные элементы схемы компьютерной сети с использованием ЛИС. Описан минимальный набор программно-аппаратных средств, необходимых для функционирования ЛИС.

5. Описана схема воздействия на защищаемый объект. Разработан подход для оценки ущерба целостности, доступности и конфиденциальности информации.Предложен вариант расчета рисков нанесения ущерба безопасности информации в результате реализации угроз целостности, доступности и конфиденциальности.Оценена эффективность применения ЛИС, как средства защиты от НСД к информации, хранимой и обрабатываемой в КС.