МОДЕЛИРОВАНИЕ ЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ С ЦЕЛЬЮ ПОВЫШЕНИЯ КАЧЕСТВА УПРАВЛЯЮЩИХ РЕШЕНИЙ В СИСТЕМАХ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

В.К. Джоган, д.т.н., доцент,
С.В. Скрыль, профессор, д.т.н.,
Д.Г. Зыбин, к.т.н., доцент
Воронежский институт ФСИН России, г. Воронеж
А.П. Сидельников, аспирант
Воронежский государственный технический университет, г. Воронеж

В настоящее время вопрос защиты информационных объектов (систем) от негативного внешнего и внутреннего воздействий нарушителей является довольно актуальным [4, 5]. Для оптимальной защиты информационных систем могут быть использованы системы-ловушки (имитаторы), называемые также ложными информационными системами (ЛИС) или обманными (ОбС).

ЛИС представляют собой программно-аппаратные средства обеспечения информационной безопасности (ИБ) (Рис. 1.), реализующие функции сокрытия и камуфляжа защищаемых информационных ресурсов, а также дезинформации нарушителей [1, 2].

В качестве основных функций, которые должны быть реализованы в перспективных ЛИС, можно выделить следующие:

- сбор и объединение данных от различных программных и аппаратных компонентов компьютерной сети;
- сканирование сетевого трафика и периодическая фиксация его состояния для последующего анализа;
- выявление источника угроз, трассировка и идентификация нарушителя;
- аутентификация и переадресация несанкционированных запросов на ложные компоненты;
- фильтрация событий;
- обнаружение действий нарушителя;

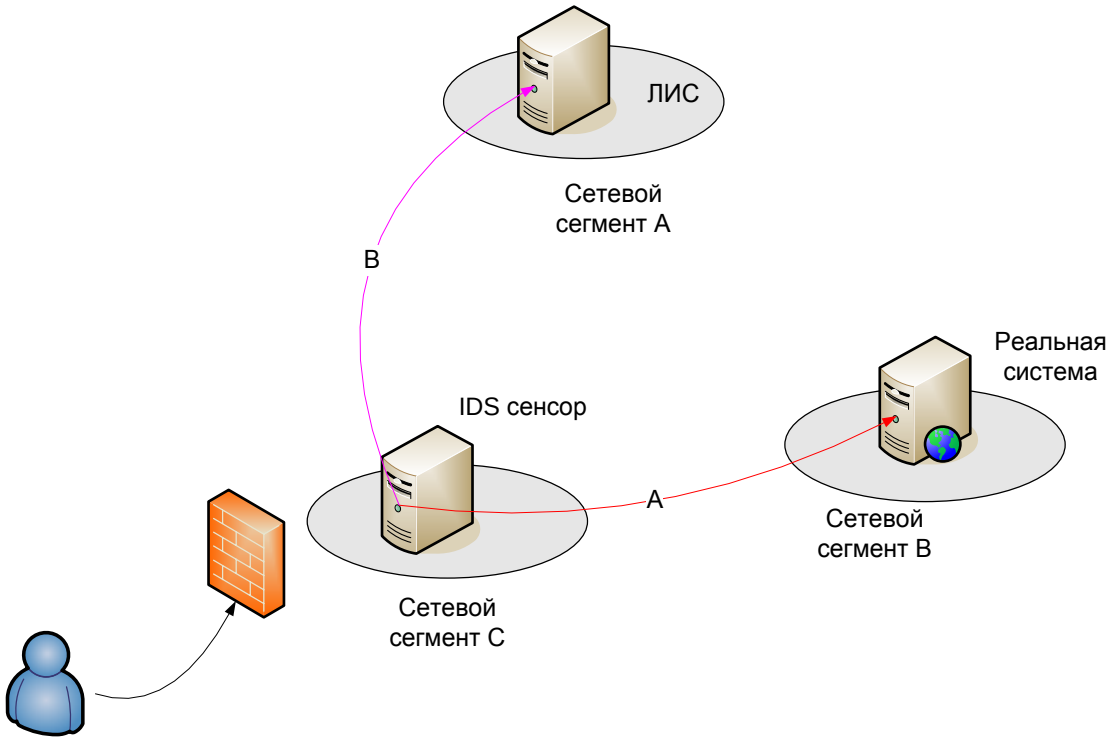

Рис. 1. Пример имитации ложных объектов в целях отвлечения злоумышленника от реальной системы ИБ.

- изоляция негативных действий нарушителя внутри ЛИС, для обеспечения невозможности нанесения вреда другим информационным объектам;
- мониторинг поведения нарушителя, контроль за его действиями, своевременное противодействие, в том числе оповещение администратора о компрометации и др.;
- формирование алгоритма действий компонентов ЛИС по имитации целевой информационной системы;
- заманивание и обман нарушителя за счёт эмуляции сетевых сегментов, серверов, рабочих станций, в том числе передаваемого трафика, и их уязвимостей, автоматическое реагирование на действия нарушителя, в том числе оповещение администратора;
- удалённое администрирование, документирование, ввод сигнатур, профилей и др;
- обеспечение удобного интерфейса с администратором безопасности (так как человеческий фактор имеет непосредственное отношение к функционированию ЛИС и как следствие к самой системе безопасности)

В общем случае ЛИС может обеспечить три уровня введения в заблуждение нарушителя [3] (Рис. 2.).

- уровень сегмента (основных компонентов целевой системы) - на данном уровне ЛИС имитирует защищаемую целевую систему в целом, и при обнаружении атаки злоумышленник перенаправляется с целевой системы на компоненты ЛИС;
- уровень хоста - данный уровень предполагает размещение компонентов

ЛИС, имитирующих отдельные хосты, в компьютерной сети целевой системы;

- уровень сервиса/приложения - в рамках хоста целевой системы каждое приложение/сервис формируется следующим образом: целевой модуль сервиса/приложения вместе с модулем обмана "вкладывается в обёртку"; в режиме санкционированного использования при вызове сервиса/приложения управление передается целевому модулю; при обнаружении несанкционированного обращения управление передается модулю обмана.

-

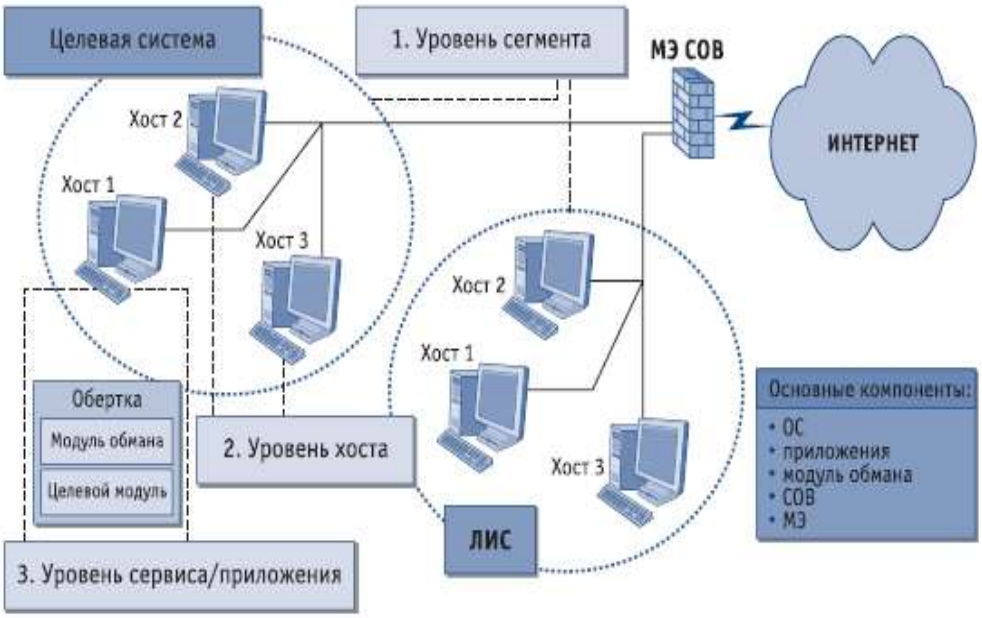

Рис 2. Уровни защиты ложной информационной системы.

Как показывает практика в использовании ЛИС и современных IPS – данные системы направлены, в основном, на предотвращение вторжений извне. Односторонняя направленность систем защиты информации (СЗИ), перекрывающая не все возможные каналы утечки информации – частая причина нанесения ущерба организациям. Зачастую в статистиках и сводках компаний, разрабатывающих подобное программное обеспечение не попадаются данные о атаках нарушителей на целевые объекты в обход имеющихся систем защиты. В качестве нарушителя в этом случае можно рассматривать инсайдера, который смог воспользоваться вычислительными средствами или же коммуникациями организации внутри защищаемого информационного периметра. Для более надежной защиты информации как от атак извне, так и от инсайдерских воздействий изнутри, считаю необходимым интегрировать дополнительные системы мониторинга и диагностирования (СМД).

Особую актуальность на современном этапе приобретает проблема разработки методологических принципов построения адаптивных СМД (АСМД), характеризуемых сложным математическим описанием и дефицитом информации, необходимой и доступной для контроля. Как

результат анализа возможностей составления адаптивных СМД, можно представить выделить упрощенную схему работы.

Упрощенная логическая схема работы систем мониторинга и диагностирования представлена на рисунке 3.

В данном случае процесс сбора и обработки информации представляют собой центральный механизм работы всей СМД. Принцип работы заключается в категорировании информации и доставки ее с устройств для дальнейшего анализа. Этими устройствами могут быть любые биометрические датчики, сканеры или снифферы (анализаторы трафика). Если анализ информации показал нарушение правил политики безопасности, то запускается кризисная программа (программа системы безопасности), нейтрализующая угрозу и выполняющая контрмеры для предотвращения утечки информации. Меры для предотвращения могут быть различны, и варьироваться только лишь политикой безопасности предприятия – от запирания дверей через систему разграничения доступа, до полной изоляции внутренней сети от внешнего мира.

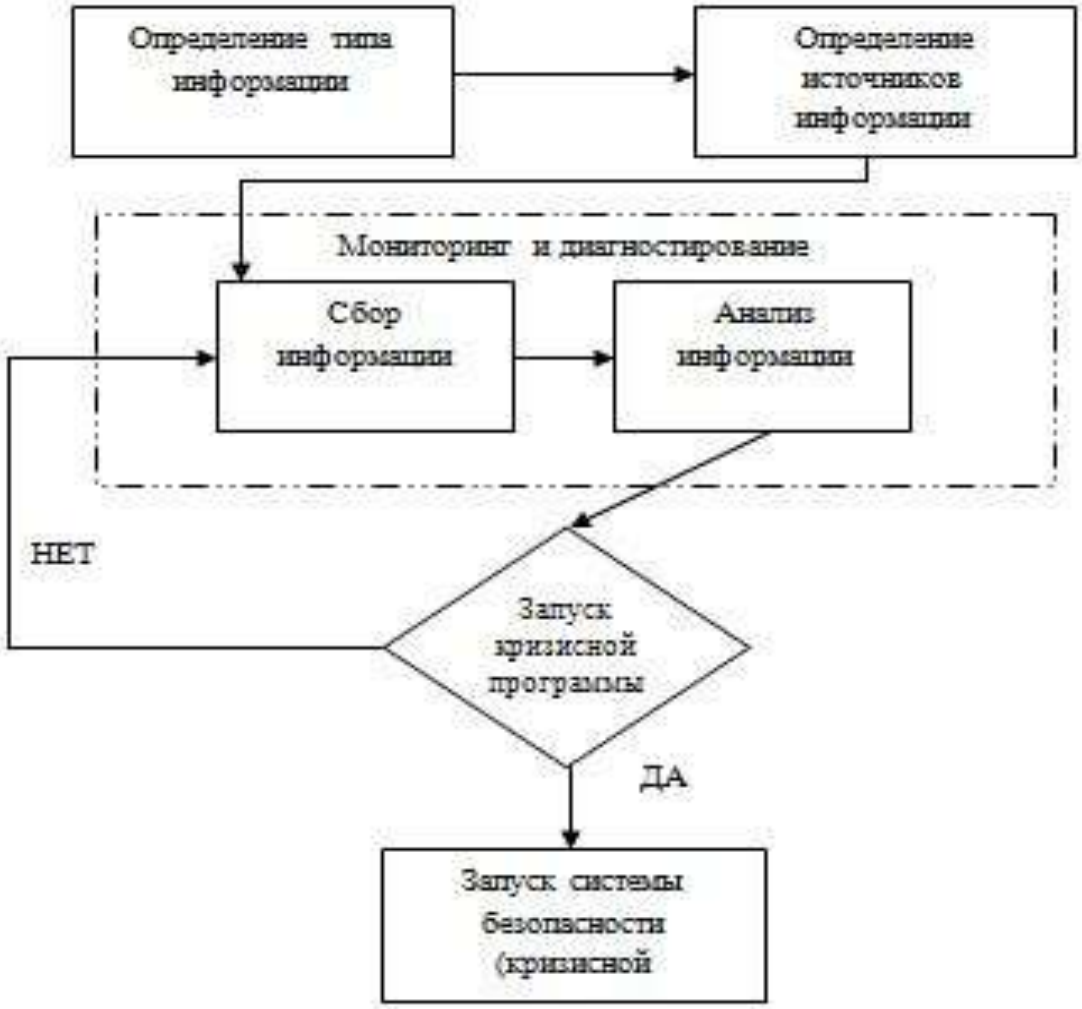

Рис. 3. Упрощенная логическая схема работы СМД.

Интеграция подсистем мониторинга и диагностирования в настоящее время обусловила необходимость создания методов и средств построения

систем мониторинга и диагностирования как единых систем на основе общих критериев, принципов построения с учетом современного уровня развития техники и достижений в смежных областях науки.

Возможность держать под контролем как внешнюю сеть, так и физический доступ инсайдеров к сетевой инфраструктуре и ее узлам – один из факторов нейтрализации успешных вторжений нарушителя. Внедрение подобных систем в систему ЛИС, является важным шагом в повышении уровня информационной безопасности.

Список используемой литературы

1. Котенко И.В., Степашкин М.В. Использование ложных информационных систем для защиты информационных ресурсов компьютерных сетей / И.В. Котенко, М.В. Степашкин // Труды СПИИРАН. - СПб: СПИИРАН, 2004. – 75 с.
2. Котенко И.В., Степашкин М.В. Системы-имитаторы: назначение, функции, архитектура иподход к реализации / И.В. Котенко, М.В. Степашкин // Труды СПИИРАН. - СПб: СПИИРАН, 2006. – 47 с.
3. Котенко И.В., Степашкин М.В. Обманные системы для защиты информационных ресурсов в компьютерных сетях / И.В. Котенко, М.В. Степашкин // Труды СПИИРАН.- СПб: СПИИРАН, 2004. - Вып.2. – 58 с.
4. Модели и алгоритмы автоматизированного контроля эффективности систем защиты информации в автоматизированных системах: монография / С.В. Белокуров, С.В. Скрыль, В.К. Джоган [и др.]. – Воронеж: Воронежский институт МВД России, 2012. – 116 с.
5. Методы и средства анализа эффективности систем информационной безопасности при их разработке: монография / С.В. Белокуров, С.В. Скрыль, В.К. Джоган [и др.]. – Воронеж: Воронежский институт МВД России, 2012. – 83 с.