ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПУТЕМ РЕАЛИЗАЦИИ МЕР ПО ОБНАРУЖЕНИЮ ВТОРЖЕНИЙ УРОВНЯ УЗЛА

Астаулов. Р.А.[1], Тимохович А.С.[2]

[1]Астаулов Роман Алексеевич – бакалавр,
направление: информационная безопасность;
[2]Тимохович Александр Степанович – кандидат педагогических наук, доцент,
кафедра безопасности информационных технологий,
Институт информатики и телекоммуникаций
Сибирский государственный аэрокосмический университет им. академика М.Ф. Решетнева,
г. Красноярск

Аннотация: *в статье проанализированы некоторые системы обнаружения вторжений (СОВ), а также приведена методика конфигурирования одной из них. На сегодняшний момент существуют разнообразные СОВ, которые способны справиться с их основной задачей: обнаружить и, по возможности, предотвратить действия злоумышленника на сетевом или локальном уровнях. Рассматриваемая СОВ OSSEC показала себя как легко настраиваемой и простой в эксплуатации. А то, что она является открытой, позволяет самостоятельно создавать правила, изменять ее конфигурацию и участвовать в разработке. Таким образом, СОВ – это современное СЗИ, способное обеспечить необходимый уровень защищенности ИС от злоумышленников, а также соответствовать требованиям регулирующих органов.*

Ключевые слова: *система обнаружения вторжений, система защиты, Ossec, информационная безопасность.*

Средства обнаружения вторжений (СОВ) – программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней. [1] В соответствии с Приказом ФСТЭК №31, защита информации посредством СОВ осуществляется от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования автоматизированной системы управления.

В таблице 1 рассмотрены основные Open Sourse СОВ уровня узла.

Таблица 1. Сравнение СОВ

СОВ / Критерий	**OSSEC**	**Samhain**	**Osiris**
поддерживаемые ОС	Linux, OpenBSD, FreeBSD, Mac OS X, Solaris, Windows	Unix, Linux, Windows	Windows, Mac OS X
поддерживаемые модули	модуль целостности файлов, модуль оповещения о вторжениях, модуль мониторинг реестра Windows	Модуль целостности файлов, мониторинг портов	Модуль целостности файлов
наличие межсетевого экрана	+	–	–
возможность распределенного управления	+	+	–
поддержка русского языка	+	–	–

Исходя из полученных данных, была выбрана СОВ OSSEC, так как в ней присутствует поддержка русского языка, она поддерживает большее количество операционных систем, а также имеет встроенный межсетевой экран. Она проста в настройке и может быть интегрирована с другими средствами защиты информации, такими как Snort или OSSIM.

Конфигурирование рассматриваемой СОВ условно можно разделить на три этапа:

1) непосредственная установка OSSEC;
2) настройка параметров;
3) тестирование работоспособности.

В ходе тестирования было установлено, что при грамотной настройке правил OSSEC способна обнаружить многие атаки на ИС, в том числе подбор паролей, сканирование портов, а также атаки, совершаемые локальными пользователями.

Таким образом, даже не сертифицированная СОВ – это хорошее СЗИ, которое способно функционировать в целях обнаружения аномального поведения в ИС, что позволяет противодействовать информационным угрозам безопасности.

Список литературы

1. Методический документ ФСТЭК России от 6 марта 2012 г. «Профили защиты систем обнаружения вторжений». [Электронный ресурс]: Режим доступа: http://fstec.ru/component/attachments/download/321 (дата обращения: 15.04.2017).
2. Обзор корпоративных IPS-решений на российском рынке. [Электронный ресурс]: Режим доступа: https://www.anti-malware.ru/IPS_russian_market_review_2013 (дата обращения: 3.05.2017).
3. Новый подход к защите информации – средства обнаружения вторжений. [Электронный ресурс]: Режим доступа: http://www.jetinfo.ru/article/ib/novyj-podkhod-k-zaschite-informatsii-sistemy-obnaruzheniya-kompyuternykh (дата обращения: 03.05.2017).