КУМАГА Н. К., ГРИГОРЬЕВЫХ А. В. ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ IDS/IPS В КОРПОРАТИВНОЙ СЕТИ УГТУ

УДК 621.394/.396.019.3, ВАК 05.13.19/2.3.6, ГРНТИ 49.33.35

Проектирование и внедрение системы обнаружения и предотвращения вторжений IDS/IPS в корпоративной сети УГТУ

Н. К. Кумага,
А. В. Григорьевых

Ухтинский государственный технический университет, г. Ухта

В статье рассматривается проектирование и внедрение системы обнаружения и предотвращения вторжений IDS/IPS для автоматизации процесса анализа, обнаружения и предотвращения вредоносной активности, а также повышения эффективности работы средств защиты информации «СрЗИ» в корпоративной сети УГТУ. В данной работе уделяется внимание исследованию предметной области, проектированию и реализации IDS/IPS на основе ПО с открытым исходным кодом.

Ключевые слова: *проектирование, системы обнаружения и предотвращения вторжений, средства защиты информации, программное обеспечение с открытым исходным кодом.*

Design and implementation of intrusion detection and prevention system IDS/IPS on the corporate network of USTU

N. K. Kumaga,
A. V. Grigor'yevykh

Ukhta State Technical University,Ukhta

This article considers the design and development of "intrusion detection and prevention system "IDS/IPS" to automate the process of analyzing, detecting and preventing malicious activities as well as improving the efficiency of information security mechanism on the corporate network of USTU. This paper focuses on the research of the subject area, the design and implementation of intrusion detection and prevention system "IDS/IPS" based on open-source programs / softwares.

Keywords: *design and implementation, information security mechanism, intrusion detection and prevention system, opensource.*

Введение

В наше время большинство учебных заведений и в том числе УГТУ, связаны с сетевыми технологиями. Эти сетевые технологии и инфраструктуры обеспечивают взаимодействие всех подразделений университета друг с другом посредством электронной почты, различных корпоративных информационных систем и даже телефонной связи. Средства обнаружения и предотвращения

вторжений все чаще становятся ключевым элементом систем безопасности для обнаружения атаки в информационной системе и корпоративной сети.

Сетевые инфраструктуры и ЛВС УГТУ постоянно расширяются, в том числе с применением Wi-Fi. В условиях широкого распространения локальных сетей УГТУ, информационные системы с обработкой персональных данных, а также спроса на доступ к глобальным сетям общего пользования крайне важно обеспечить сетевую безопасность и обеспечить безопасный доступ сотрудников и студентов к сетевым ресурсам в любое время.

В УГТУ на данный момент, для обеспечения безопасности или защиты информации используются средства промежуточного доступа (Proxy Server), межсетевые экраны (Firewall) и средства антивирусной защиты. Использование только этих механизмов защиты информации не позволяет полноценно и эффективно обеспечить выявление и предотвращение несанкционированной и вредоносной активности в сети УГТУ. Из этого вытекают следующие проблемы:

1. Несанкционированный доступ к сети и системам
2. Несанкционированное использование IP-телефонии
3. Взлом сайтов и веб-приложений
4. Шифровка компьютеров пользователей с целью вымогания денег.

Целью данного проекта является проектирование и внедрение системы обнаружения и предотвращения вторжений для автоматизации процесса анализа, обнаружения и предотвращения вредоносной активности на базе программы с открытым исходным кодом (opensource), а также повышение эффективности работы средства защиты информации «СрЗИ» в корпоративной сети УГТУ.

Предпроектное исследование

В настоящее время сеть УГТУ построена на базе нескольких серверов, контроллеров, домена ugtu, маршрутизаторов Cisco 1800, коммутаторов Cisco и DLink. Общая пропуская способность сети составляет 10/100 Мбит/с и позволяет осуществлять полноценную загрузку сервера системы и использовать современное ПО. В локальной сети УГТУ находится порядка тысячи рабочих станций. Обеспечение безопасности этой сетевой инфраструктуры выполняется следующим образом:

− Использования средства промежуточного доступа (Proxy Server) и межсетевые экраны (Firewall);

− Средства аутентификации и авторизации пользователей «User Authentication Facilities – UAF);

− Средства антивирусной защиты;

− Средства физического и программного разграничения доступа к распределенным и разделяемым информационным ресурсам;

− Реализацией технологий VPN (Virtual Private Network) на очень критически место на примере в бухгалтерии.

Для обеспечения безопасности в сети УГТУ недостаточно только этих механизмов и средств защиты информации.

Для повышения защиты корпоративной сети ИС УГТУ необходимы сетевые ресурсы от атак извне и дополнение уже существующих технологий, поэтому была поставлена задача внедрения системы обнаружения и предотвращения вторжений IDS/IPS.

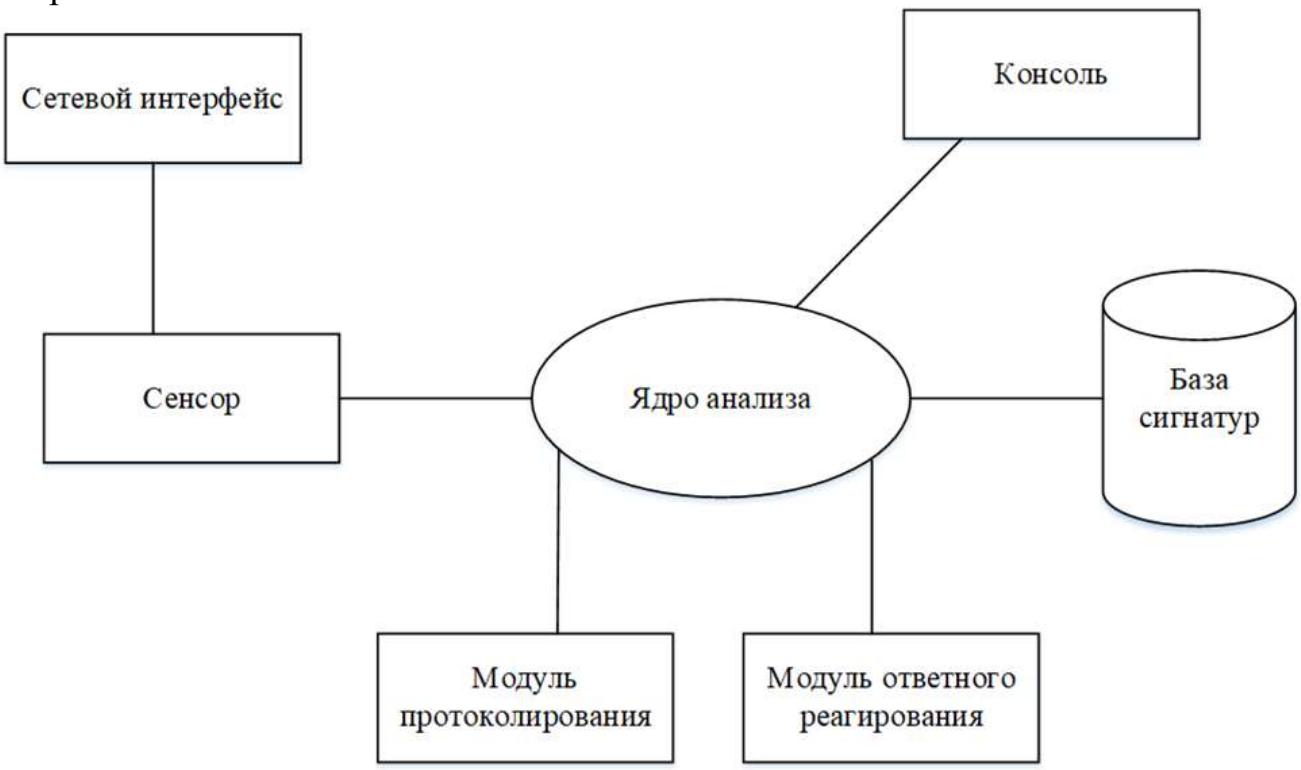


Рисунок 1. Структурная схема IDS

1. Датчики – сенсоры, используются для мониторинга событий, связанных с безопасностью защищаемой системы;
2. Анализаторы – выполняют анализ подозрительной активности на основе информации, полученной от датчиков (сенсоров). Затем генерируют отчёты с результатами анализа и управляют процессами реагирования на выявленные инциденты;
3. Хранилище – обеспечивает сбор данных, о событиях и анализ результатов;
4. Консоль управления – с её помощью оператор конфигурирует СОВ, производит анализ инцидентов, следит за состоянием защищаемой системы.

Функционирование систем IDS во многом аналогично межсетевым экранам: сенсоры получают сетевой трафик, а ядро путём сравнения полученного трафика с записями имеющейся базы сигнатур атак пытается выявить следы попыток несанкционированного доступа. Модуль ответного реагирования представляет собой опциональный компонент, который может быть использован для оперативного блокирования угрозы: например, может быть сформировано правило для межсетевого экрана, блокирующее источник нападения. [1]

Обзор аналогов и литературы

В настоящее время, на рынке товаров и услуги по ИБ существуют огромное количество систем для обнаружения вторжений. Среди этих систем есть коммерческих (Платные) и есть бесплатные системы с открытым исходным кодом. В России Существуют несколько программно-аппаратных СОВ от крупных компании рынка ИБ, таких как Cisco, MacAfee, infotecs, Positive technologies и других, которые имеют сертификаты ФСТЭК. [2]

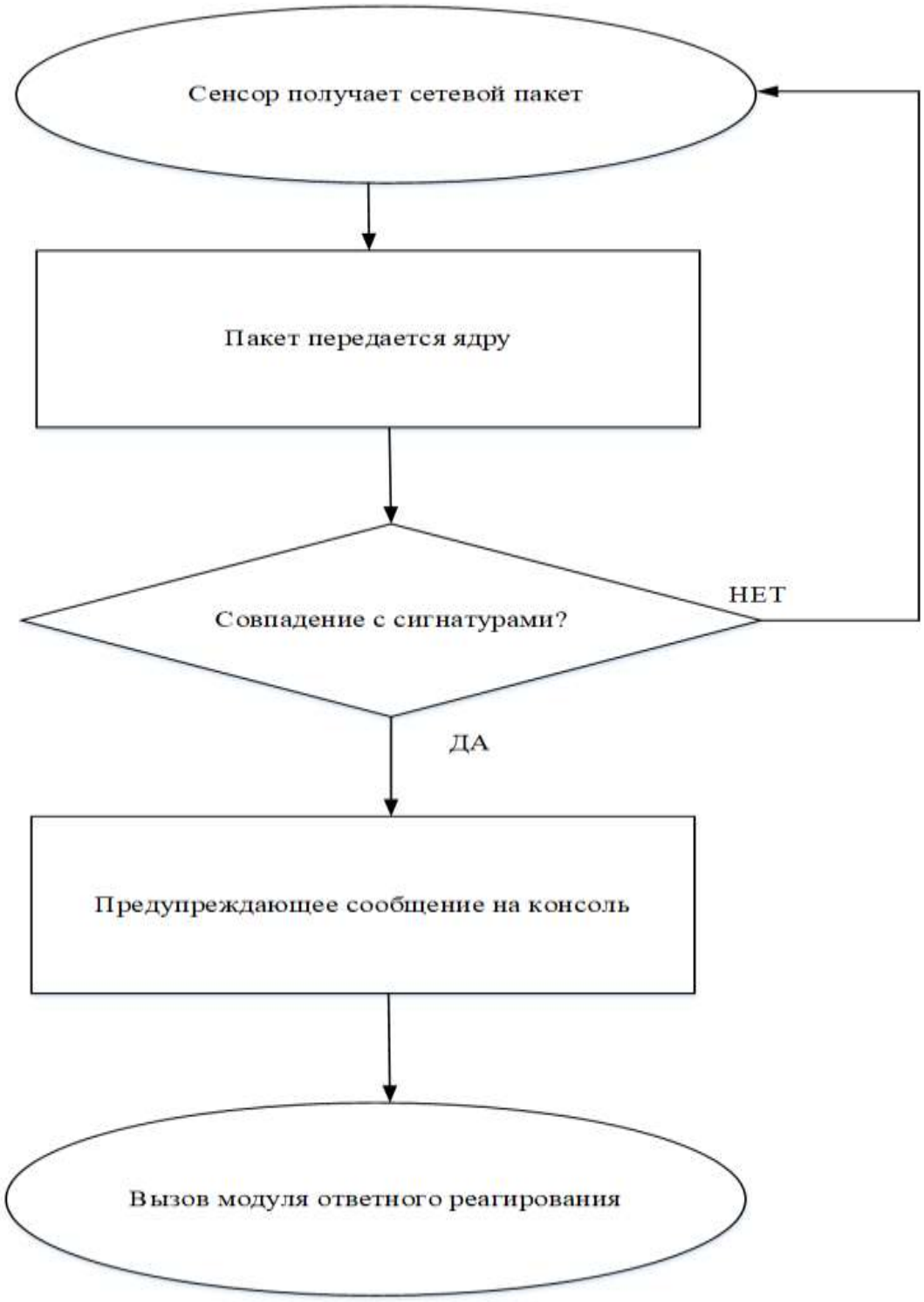


Рисунок 2. Схема работы IDS

На рынке ещё являются бесплатными такие программные комплексы как: Snort, Suricata, Bro, OSSEC, Easy IDS, Open Source Tripwire.

Первый рассматриваемый аналог – приложение Snort. Snort является классической IDS уровня сети и анализирует трафик на совпадение с базой правил (фактически с базой сигнатур). Т.е., данная система ищет известные нарушения. На базе Snort реализовано много известных коммерческих решений, в том числе русских. Помимо работы с базой сигнатур, построенная на базе Snort IDS, вполне может иметь в своём составе эвристические, нейросетевые и подобные модули обнаружения. Как минимум, существует в рабочем виде статистический детектор аномалий для Snort. [4]

Второй рассматриваемый аналог – Suricata. Suricata также, как и Snort является системой уровня сети. У данной системы есть несколько особенностей:

Базы сигнатур совместимы со Snort.

Оценивает не только сетевой/транспортный уровень, но работает и на уровне прикладных протоколов.

Есть возможность реализовывать правила на Lua, интерпретируемом языке, что расширяет диапазон возможностей.

Можно анализировать трафик между двумя хостами, в целом, а не только отдельные пакеты/соединения. Это позволяет, например, обнаруживать попытки подбора паролей.

Есть подсистема IP reputation, позволяющая присваивать "уровень репутации" каждому IP адресу. Т.е. эта система, хотя и обнаруживает известные нарушения, также как и предыдущая, обладает большей адаптивностью и возможностью обучаться (уровень репутации хоста может изменяться в процессе работы системы и влиять на принятие ей решения).

Третий рассматриваемый аналог – Bro.

Платформа для создания IDS уровня сети. Является гибридной системой, с упором на обнаружение известных нарушений. Работает на транспортном, сетевом уровне и уровне приложений. Поддерживает свой язык сценариев.

Имеется возможность обнаружения аномалий, например, множественное подключение к сервисам на разных портах — не свойственное для нормального узла поведение, которое будет обнаружено. [7]

Это реализовано, во-первых, на основе проверок передаваемых данных на нормальность (например, TCP-пакет со всеми установленными флагами, наверное тут что-то не то, несмотря на то, что он корректен). Во-вторых, на базе политик, описывающих как должна функционировать сеть в норме. Bro не только обнаруживает атаки, но также помогает при диагностике сетевых проблем (заявленный функционал).

Таблица 2. Сравнение прямых аналогов

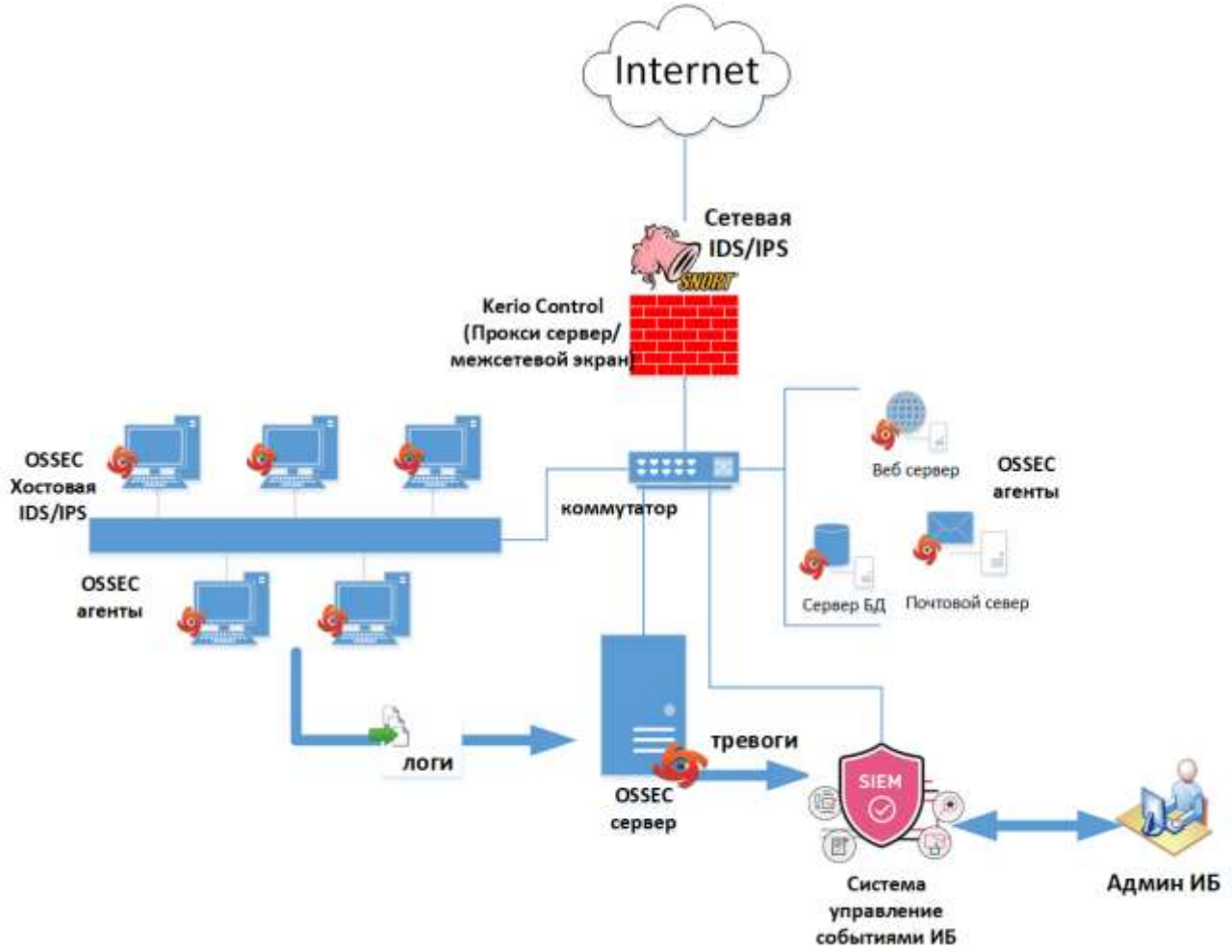
Критерии / Функции	Snort	OSSEC	Suricata	Bro(Zeek)	Samhain
ПО	+	+	+	+	+
ПАК	-	-	-	-	-
Сетевая	+	-	+	+	-
Хостовая	-	+	+	-	+
Гибридная	-	-	-	+	-
Сигнатурный	+	+	+	+	+
Поиск аномалий	+	+	-	-	+
Сертификация	-	-	-	-	-
Полнота Документа	+	+	+	+	+
Техническая Поддержка	-	-	-	-	-
Активный режим	+	-	+	-	-
Постоянная поддержка сообщества	+	+	+	+	-
Агент – сервер	-	+	-	-	-
Смешать с Kerio proxy	+	-	-	-	-

Разработка схемы внедрения

Для максимальной эффективности развертывания системы IDS/IPS в корпоративной сети УГТУ, необходимо проанализировать архитектуру и конфигурацию текущей сети и наметить точки установки сенсоров IDS/IPS и другие дополнительные системы. Для этих целей нужны схемы внедрения.

Для внедрения системы IDS/IPS в корпоративной сети «УГТУ» были использованы следующие подсистемы:

1. Ansible
2. Snort IDS/IPS
3. OSSEC IDS/IPS
4. SIEM-Система (Elasticsearch)



Ansible – это система управления конфигурациями с открытым исходным кодом, написанным на языке программирования Python, которое помогает автоматизировать настройки и быстро развертывать ПО и обслуживания удаленных серверов.

Краткий словарь терминов Ansible

− Control Machine (или Node): ведущая система, в которой установлен Ansible и откуда он может подключаться к нодам и выполнять на них команды.

− Нода: сервер, управляемый Ansible.

− Файл инвентаря: файл, который содержит информацию о серверах, которыми управляет Ansible, обычно находится в /etc/ansible/hosts.

− Плейбук (Playbook): файл, содержащий серию задач, которые нужно выполнить на удаленном сервере.

− Роль: коллекция плейбуков и других файлов, которые имеют отношение к цели (например, к установке веб-сервера).

− Play: полный набор инструкций Ansible. В play может быть несколько плейбуков и ролей, включенных в один плейбук, который служит точкой входа.

Реализация и демонстрация системы на виртуальном стенде

Для реализации и демонстрации обнаружения атак системой и отправления тревоги к SIEM-система, был разработан виртуальный стенд в программе Oracle

VirtualBox с установкой следующие операционной системы: CenstOS, Ubuntu, Windows 10 и Kali Linux.

2 CentOS сервер для установки программы Ansible и Snort IDS, Ubuntu ОС для установки SIEM-Система, Windows 10 для установки OSSEC IDS, а Kali Linux для компьютера злоумышленника. С помощью Kali Linux имитировать вторжение или атаки.

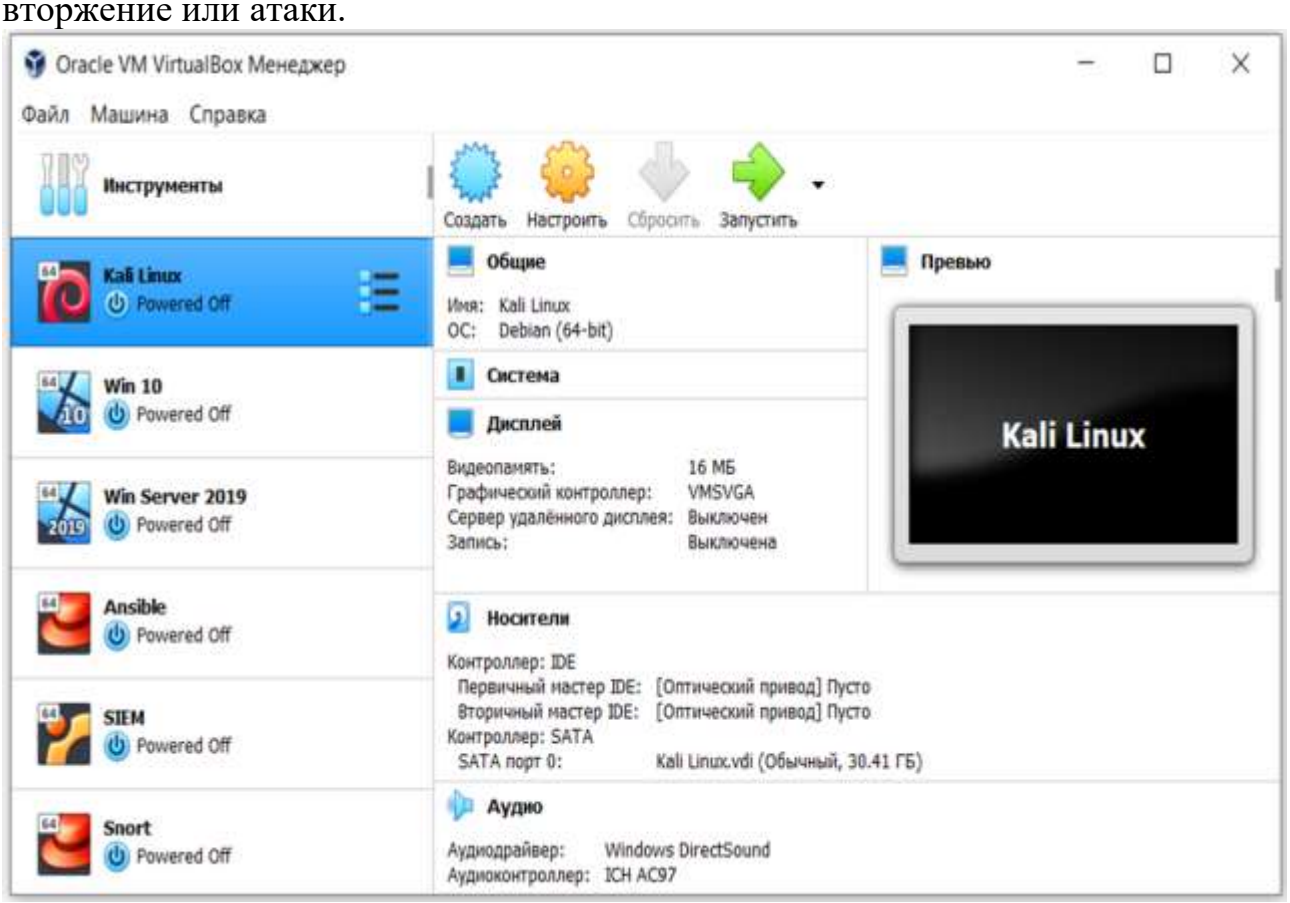


Рисунок 4. Перечень виртуальных машин, созданных в Oracle VirtualBox

Заключение

В данной статье дано краткое описание работ по проектированию и внедрению системы обнаружения, предотвращения вторжений “IDS/IPS” в корпоративной сети УГТУ. Помимо вышеописанных пунктов, процесс проектирования системы включил в себя следующие этапы:

– анализ состояния защищенности сети УГТУ от несанкционированных вторжений;

– изучение назначения, состава, принципов функционирования и организации предмета проектирования;

– изучение аналогов проектируемого объекта;

– предпроектное обследование предметной области;

– осуществлен выбор и описание средств проектирования;

– выполнена разработка технического задания;

– разработка стенда из виртуальных машин для демонстрации работы системы обнаружения вторжений;

– разработка скрипта автоматизации процесса установки и конфигурирования системы обнаружения вторжений и SIEM-Система на основе Ansible;

– тестирование работы системы обнаружения вторжений на стенде виртуальных машин.

Список использованных источников и литературы

1. Системы и методы обнаружения вторжений: современное состояние и направление совершенствования [Электронный ресурс]. – Режим доступа: http://citforum.ru/security/internet/ids_overview/ (дата обращения: 02.06.2021).

2. ФСТЭК России. Информационное письмо об утверждении требований к системам обнаружения вторжений [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/118-tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/prikazy/394-informatsionnoe-pismo-fstek-rossii (дата обращения: 02.06.2021).

3. Безопасность сетей [Электронный ресурс]. – Режим доступа: https://intuit.ru/studies/courses/102/102/lecture/2995 (дата обращения: 01.04.2021).

4. Официальный сайт проекта Snort [Электронный ресурс]. – Режим доступа: https://www.snort.org/ (дата обращения: 01.06.2021).

5. Инструменты безопасности с открытым исходным кодом [Электронный ресурс]. – Режим доступа: https://intuit.ru/studies/courses/7/7/lecture/226?page=5 (дата обращения: 04.06.2021).

6. Аудит состояния информационной безопасности на предприятии [Электронный ресурс]. – Режим доступа: https://intuit.ru/studies/courses/563/419/lecture/9583 (дата обращения: 04.06.2021).

7. Официальный сайт проекта Bro [Электронный ресурс]. – Режим доступа: https://zeek.org/ (дата обращения: 04.06.2021).

List of references

1. Systems and methods of intrusion detection: current state and directions of improvement, http://citforum.ru/security/internet/ids_overview/, accessed June 02, 2021

2. FSTEC of Russia. Information letter on the approval of requirements for intrusion detection systems, https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/118-tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/prikazy/394-informatsionnoe-pismo-fstek-rossii, accessed June 02, 2021.

3. Network security, https://intuit.ru/studies/courses/102/102/lecture/2995, accessed April 01, 2021

4. Official website of the Snort project, https://www.snort.org/, accessed June 01, 2021.

5. Open source security tools, https://intuit.ru/studies/courses/7/7/lecture/226?page=5, accessed June 04, 2021.

6. Audit of the state of information security at the enterprise, https://intuit.ru/studies/courses/563/419/lecture/9583, accessed June 04, 2021.

7. Official website of the Bro project, https://zeek.org/, accessed June 04, 2021.