|  |  |
| --- | --- |
| СОГЛАСОВАНО | УТВЕРЖДЕНО |
| Главный конструктор  АО «Окенит»  (подпись) Н.В. Фамилия  07.07.2024 | Генеральный директор  ОАО «Компания»  (подпись) Г.Е. Груздев  07.07.2024 |

АО «ОКЕНИТ»

Программное средство

Система обнаружения вторжений

«СОВ УС»

643.12345678.12345-01 90 01-ЛУ

ЛИСТ УТВЕРЖДЕНИЯ

Листов 1

|  |  |
| --- | --- |
|  | СОГЛАСОВАНО |
|  |  |
|  | Заместитель начальника отдела №1  АО «Компания»  (подпись) Г.Е. Груздев  07.07.2024 |

2024

УТВЕРЖДЕНО

643.12345678.12345-01 90 01-ЛУ

ОКЕНИТ

Система обнаружения вторжений

«СОВ УС»

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

643.12345678.12345-01 90 01

Листов 18

2024

**АННОТАЦИЯ**

Настоящее Техническое Задание (ТЗ) определяет назначение, общие и специальные требования к системе обнаружения вторжений, предназначенной для анализа сетевого трафика, выявления подозрительных действий и потенциальных атак, а также предоставления средств для оперативного реагирования на угрозы информационной безопасности.

**Содержание**

[ВВЕДЕНИЕ 3](#_Toc179834871)

[1. ОСНОВАНИЯ ДЛЯ РАЗРАБОТКИ 4](#_Toc179834872)

[2. НАЗНАЧЕНИЕ РАЗРАБОТКИ 5](#_Toc179834873)

[3. ТРЕБОВАНИЯ К ПРОГРАММЕ ИЛИ ПРОГРАММНОМУ ИЗДЕЛИЮ 6](#_Toc179834874)

[3.1. Функциональные требования 6](#_Toc179834875)

[3.2. Условия эксплуатации: 9](#_Toc179834876)

[3.3. Требования к информационной и программной совместимости: 10](#_Toc179834877)

[3.4. Требования к маркировке и упаковке: 11](#_Toc179834878)

[3.5. Требования к транспортированию и хранению: 11](#_Toc179834879)

[3.6. Специальные требования: 11](#_Toc179834880)

[4. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ 13](#_Toc179834881)

[5. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ 14](#_Toc179834882)

[6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ 15](#_Toc179834883)

[Лист регистрации изменений 17](#_Toc179834884)

# ВВЕДЕНИЕ

Наименование: система обнаружения вторжений «СОВ УС»

Разрабатываемая система обеспечит возможность выявления и предотвращения сетевых атак и угроз информационной безопасности в реальном времени

Настоящее техническое задание является основным документом, определяющим требования к разрабатываемой системе обнаружения вторжений (IDS/IPS) и ожидаемые характеристики готового продукта.

# 1. ОСНОВАНИЯ ДЛЯ РАЗРАБОТКИ

Основанием для разработки программного средства являются следующие документы:

1. Государственный контракт №1/88-00-55-535 от 01.07.2024 года на разработку и эксплуатацию системы обнаружения вторжений;
2. Договор №80085 от 01.07.2024 года на разработку и эксплуатацию системы обнаружения вторжений между АО «Окенит» и ОАО «Компания».

Организация, утвердившая документ: ОАО «Компания»

Дата утверждения документа: 07.07.2024 г.

Шифр темы разработки: 643.12345678.62.01-01 90 01

# 2. НАЗНАЧЕНИЕ РАЗРАБОТКИ

Назначение разработки новой IDS/IPS системы заключается в создании инструмента для защиты сетевой инфраструктуры от атак.

1. Обнаружение угроз в реальном времени: IDS/IPS отслеживает и анализирует сетевой трафик, помогая обнаруживать потенциальные угрозы, такие как вредоносное ПО, атаки на уязвимости, попытки несанкционированного доступа и другие формы сетевых атак.
2. Предотвращение сетевых атак: система может блокировать подозрительный трафик или ограничивать доступ атакующим, тем самым предотвращая дальнейшее распространение угрозы или атаку на уязвимые системы.
3. Анализ и мониторинг трафика: система собирает подробные данные о сетевом трафике, выявляют аномалии и предоставляют возможность для глубокого анализа инцидентов безопасности. Это помогает выявлять не только конкретные угрозы, но и следить за общим поведением сети.
4. Интеграция с другими системами безопасности: IPS/IDS могут работать в связке с другими инструментами безопасности, такими как межсетевые экраны, SIEM и системы управления уязвимостями, предоставляя более полную картину угроз и повышая эффективность защиты.
5. Предотвращение финансовых потерь: успешные кибератаки могут привести к значительным финансовым потерям из-за простоя бизнеса, утраты данных, штрафов за нарушение норм или повреждения репутации. IPS помогает минимизировать эти риски, предотвращая атаки до того, как они нанесут ущерб.

# 3. ТРЕБОВАНИЯ К ПРОГРАММЕ ИЛИ ПРОГРАММНОМУ ИЗДЕЛИЮ

**3.1. Функциональные требования**

1. **Обнаружение угроз в реальном времени**:

- Система должна анализировать весь входящий и исходящий трафик в режиме реального времени между внутренней сетью компании и внешними сетями, а также между различными сегментами внутренней сети (протоколы HTTP, HTTPS, DNS, SMTP, FTP, SSH, Telnet, RDP, TCP, UDP, ARP).

- Обнаружение угроз должно основываться на сигнатурах (известные атаки – базы Emerging Threats и Snort) и обнаружении аномалий в поведении сетевого трафика на основе анализа шаблонов обычной активности, что позволяет выявлять потенциальные атаки типа zero-day или неизвестные угрозы.

2. **Предотвращение угроз**:

- Система должна иметь возможность блокировать вредоносный трафик на основании обнаруженных угроз. Например, если система идентифицирует попытку SQL-инъекции через HTTP-запрос на веб-сервер, IPS должна автоматически блокировать запрос на уровне шлюза.

- Блокировки могут быть настроены в зависимости от типа угрозы, конкретного сегмента сети (например, блокировка на уровне внутреннего сегмента или между DMZ и внутренней сетью), или политики безопасности (блокировка всех подозрительных запросов или только специфических типов).

3. **Гибкость настройки правил**:

- Система должна позволять создавать и настраивать собственные правила для обнаружения специфических угроз, которые могут быть уникальны для инфраструктуры или бизнес-процессов организации. Правила записываются в виде файлов с расширением .rule, пути к пользовательским правилам указываются в конфигурационном файле с расширением .conf.

- Привила должны иметь возможность гибкой настройки фильтрации по типу трафика (например, HTTP, FTP, DNS).

4. **Анализ различных протоколов**:

- Система должна анализировать как заголовки пакетов, так и содержимое данных, проходящих через сеть для идентификации атак, маскирующихся под обычный трафик. Проверка осуществляется для таких протоколов, как HTTP, HTTPS, DNS, SMTP, FTP, SSH, Telnet, RDP, TCP, UDP, ARP.

5. **Сбор и логирование данных**:

- Система должна фиксировать все события, связанные с обнаружением угроз, включая детектированные атаки, действия системы (блокировки, уведомления), а также информацию о заблокированных пакетах и соединениях.

- Логи должны содержать подробную информацию о каждом событии, включая: время и дату инцидента, IP-адреса источника и назначения, сетевой протокол, тип обнаруженной атаки или аномалии, действие, предпринятое системой (блокировка, уведомление).

6. **Архитектура программы:**

**Входные данные:**

- Сетевой трафик (сетевые пакеты).

- Правила и сигнатуры атак (Snort, Emerging Threats).

**Выходные данные:**

- Логи и отчеты об угрозах (в формате JSON).

- Записи сетевого трафика (PCAP).

- Уведомления о детектированных угрозах.

- Результаты работы IPS — заблокированный вредоносный трафик.

Архитектура программы представлена на рисунке 1:



Рисунок 1 – Архитектура программы

- Модуль захвата трафика прослушивает сетевой трафик, поступающий на сетевой интерфейс, как от внешней (сеть интернет), так и от внутренней сетей (локальный сегмент сети).

- Модуль декодирования отвечает за разбор сетевого трафика на уровне пакетов, извлечение информации о протоколах, сегментации данных.

- Модуль потоковой сборки занимается группировкой пакетов в сессии, что позволяет анализировать состояния соединений и контекст трафика.

- Модуль анализа сигнатур отвечает за сопоставление сетевых событий с базой сигнатур для выявления известных атак.

- Модуль анализа аномалий отвечает за обнаружение необычного поведения в сети, которое может указывать на новые, неизвестные угрозы.

- Модуль предотвращения атак занимается предотвращением атак в реальном времени путём блокирования вредоносного трафика до его достижения целевой системы (объекта внутреннего сегмента сети).

- Модуль записи и логирования отвечает за регистрацию выявленных угроз и событий безопасности, запись их в память локального компьютера или передачу в системы управления событиями (SIEM).

**3.2. Условия эксплуатации:**

Для защиты аппаратуры от бросков напряжения и коммутационных помех должны применяться сетевые фильтры.

Для оптимального функционирования средства защиты условия окружающей среды не критичны. Средство должно эксплуатироваться в офисных условиях: 22-25°С.

Для обеспечения бесперебойной работы системы IDS/IPS рекомендуется наличие квалифицированного персонала с навыками управления системами сетевой безопасности, анализа угроз и реагирования на инциденты.

Система должна находиться под постоянным контролем в режиме 24/7, с возможностью немедленного реагирования на инциденты. Для этого могут использоваться как автоматизированные системы оповещения, так и команда специалистов, ответственная за мониторинг и управление системой безопасности.

Система должна поддерживать механизмы резервирования, включая резервные источники питания (UPS), резервирование критических компонентов (двойные сетевые адаптеры, резервные серверы), а также автоматический перезапуск системы в случае сбоя. Это обеспечит отказоустойчивость системы и минимизирует время простоя.

В случае сбоя система должна поддерживать возможность автоматического восстановления работоспособности с сохранением данных логирования и состояния сети до сбоя. Среднее время восстановления (MTTR) должно составлять не более 30 минут.

**3.3. Требования к информационной и программной совместимости:**

* Процессор 2 ядра 2 ГГц и выше (с поддержкой инструкций SSE2).
* Оперативная память: 4 ГБ и выше.
* 20 ГБ и выше свободного места на жестком диске.

Программные средства защиты должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

* Astra Linux 1.6 SE, 1.7 SE;
* Ubuntu 22.04.1 LTS, 24.04.1 LTS.

Библиотеки, требуемые для установки:

- libjansson, libpcap, libpcre2, libyaml, zlib

Утилиты, требуемые для установки:

- make, gcc (или clang), pkg-config, rustc, cargo

**Ограничения:**

При обработке больших объемов сетевого трафика система должна иметь возможность работы в условиях высокой нагрузки без снижения производительности. Ограничение на объем входящего трафика, который может быть обработан, зависит от доступных аппаратных ресурсов (оперативной памяти, процессора, пропускной способности сетевых интерфейсов).

Обновления баз сигнатур и правил детектирования должны проводиться регулярно, без значительного увеличения нагрузки на систему.

**3.4. Требования к маркировке и упаковке:**

Комплект поставки: формуляр, эксплуатационная документация, копия сертификата соответствия, программа и ключ на материальном носителе (CD-накопитель), лицензионное соглашение. Требования к маркировке: обязательное наличие на носителе знака соответствия, обозначения, названия, фирма, дата.

**3.5. Требования к транспортированию и хранению:**

Транспортировка должна обеспечивать защиту носителя информации от ударов и механических повреждений. Хранение носителя информации производится в сухом помещении, не допускающем попадание на его поверхности влаги, солнечных лучей и летучих веществ, которые могут привести к потере данных на диске.

**3.6. Специальные требования:**

1. Средство защиты информации по окончании работ и тестирования должно быть сертифицировано ФСТЭК России:

- Приказ ФСТЭК России № 76 от 02.06.2020 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к технической защиты информации и средствам обеспечения безопасности информационных технологий»

2. При разработке изделия необходимо придерживаться методических рекомендаций, которые направлены на предотвращение влияния на функции безопасности операционной системы специального назначения Astra Linux Special Edition и Ubuntu 22.04/24.04 в процессе проектирования, разработки и эксплуатации программного обеспечения.

# 4. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ

Ориентировочная экономическая эффективность не рассчитывается.

Предполагаемая годовая потребность продукта: 20 лицензий в год.

Зарубежные и отечественные аналоги: Suricata, Snort и пр.

Преимущества по сравнению с аналогами:

- Интеллектуальное обнаружение угроз: анализ поведения и машинное обучение.

- Модульная интеграция и совместимость: гибкость в адаптации к различным средам.

- Динамическое и настраиваемое управление правилами: адаптация под специфические угрозы.

- Запуск в многопоточных сценариях: возможность обрабатывать больше трафика одномоментно.

# 5. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ

Стадии разработки: формирование требований, разработка концепции, техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие, сопровождение.

Этапы

- Разработка

- Опытная эксплуатация

- Передача в постоянную эксплуатацию

Документация

Предварительный состав ПД:

* Описание применения 643.12345678.12345-01 31 01;
* Формуляр 643.12345678.12345-01 30 01;
* Спецификация 643.12345678.12345-01;
* Техническое задание 643.12345678.12345-01 90 01;
* Программу и методику испытаний 643.12345678.12345-01 51 01;
* Текст программы 643.12345678.12345-01 12 01;
* Руководство оператора 643.12345678.12345-01 34 01;
* Технические условия 643.12345678.12345-01 92 01;
* Пояснительная записка 643.12345678.12345-01 81 01;
* Ведомость эксплуатационных документов

643.12345678.12345-01 20 01;

* Описание программы 643.12345678.12345-01 13 01.

# 6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

Разработка

В процессе разработки программного средства осуществляется постоянный контроль его качества. Разработка включает следующие этапы:

* Анализ требований и подготовка технического задания;
* Проектирование архитектуры системы и компонентов;
* Написание и отладка программного кода;
* Тестирование на каждом этапе разработки (модульное, интеграционное и системное тестирование);
* Подготовка документации (руководство пользователя, техническая документация).

По завершении каждого этапа разработки проводится внутреннее тестирование разработчиком с целью проверки выполнения функциональных требований и выявления возможных ошибок.

Для фиксации результатов на этапе разработки составляется технический отчёт, включающий описание выполненных задач, выявленных дефектов, способы их устранения, а также результат промежуточного тестирования.

Опытная эксплуатация

Опытная эксплуатация проводится после завершения разработки и предварительного тестирования программного средства в условиях, максимально приближенных к реальной эксплуатации.

В рамках данного этапа:

* Устанавливается тестовая версия программы в инфраструктуре Заказчика;
* Проводится проверка функциональности программного обеспечения в реальных рабочих условиях, с использованием реальных данных;
* Анализируются показатели производительности системы, выявляются и устраняются недостатки, не обнаруженные на этапе разработки;
* Проводится дополнительное обучение персонала, если это предусмотрено условиями договора.

По завершении этапа опытной эксплуатации составляется акт приёмки опытной эксплуатации, в котором фиксируются выявленные недостатки (если такие имеются), а также подтверждается готовность системы к вводу в постоянную эксплуатацию.

Передача в постоянную эксплуатацию

Приемо-сдаточные испытания должны проводиться в сроки с 01.09.2024 года по 31.12.2024 года.

Приемо-сдаточные испытания программы должны проводиться согласно разработанной не позднее 15.11.2024 года Исполнителем и согласованной Заказчиком Программы и методик испытаний. Виды, состав, объем, и методы испытаний подсистемы должны быть изложены в программе и методике испытаний, разрабатываемой в составе рабочей документации.

Сдача-приёмка осуществляется комиссией, в состав которой входят представители Заказчика и Исполнителя. По результатам приемки подписывается акт приёмочной комиссии.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Лист регистрации изменений** | | | | | | | | | |
| Номер листов (страниц) | | | | | Всего листов (страниц) | № докум | Входящий номер сопроводит. документа и дата | Подпись | Дата |
| Изм | изменен | заменен | новых | аннулир |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |