

ООО Дигилабс

ОГРН: 1207700443532, ИНН: 7707445960, КПП: 770701001

## Программный продукт **ХантерЛог (HunterLog)**

### Описание функциональных характеристик программного обеспечения

(для целей проведения экспертной проверки в Экспертном совете при  
Минцифры России)

Москва  
2022 г.

## Оглавление

1.	ОБЩИЕ СВЕДЕНИЯ .....	3
2.	ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	3
3.	ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ .....	5
	Active Directory: .....	5
	Раздел DNS & DHCP .....	6
	Раздел Exchange: .....	7
	Раздел Локальный компьютер: .....	9
	Раздел Linux: .....	9
	Раздел VMware .....	10
	ESXi .....	10
	vCenter .....	11
	Раздел NetFlow.....	11
	Раздел VPN.....	11
4.	АРХИТЕКТУРА .....	13
5.	ЮРИДИЧЕСКАЯ ИНФОРМАЦИЯ .....	14
	Авторские права.....	14
	Содержание документа .....	14

## 1. ОБЩИЕ СВЕДЕНИЯ

ХантерЛог – программный продукт (далее также – «Продукт»), является централизованной системой аудита для предприятий любого размера. Обеспечивает эффективный сбор, обработку и хранение событий с поддерживаемых сервисов. Данный продукт обеспечивает возможность оперативного доступа к информации, объединив ее в одном источнике, тем самым повышая ценность, а также удобство ее последующей обработки. Современный и практичный интерфейс гарантирует простоту использования всех функциональных возможностей.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Раздел содержит определения основных терминов, используемых в настоящем документе.

Термин	Определение
Веб-консоль	Веб-интерфейс пользователя, который предоставляет доступ ко всем данным мониторинга.
Root cause	Реальная причина проблемы (первопричина).
Active Directory (AD)	Служба каталогов, разработанная Microsoft для доменных сетей Windows.
Group Policy Objects	Набор политик, называемые объектами групповой политики. Служит для централизованного управления пользователями и компьютерами в домене.
DNS	Система, преобразующая человекочитаемые доменные имена в IP-адреса, понимаемые машиной.
DHCP	Протокол прикладного уровня, который помогает назначать IP-адреса устройствам при подключении к серверу. Протокол DHCP автоматизирует выдачу адресов, а также их передачу следующим пользователям после отключения устройств или их перехода из одной подсети в другую.
Exchange	Программный продукт для обмена сообщениями и совместной работы, корпоративная почта.
OWA	веб-клиент для доступа к серверу совместной работы Microsoft Exchange.
ActiveSync	Программа, позволяющая установить синхронизированную связь между мобильным устройством и персональным компьютером, а также сервером, работающим под управлением Microsoft Exchange Server
DAG (Database Available Group)	Технология обеспечения отказоустойчивости баз данных почтовых ящиков.
PowerShell	Программа автоматизации задач и управления конфигурацией от Microsoft, состоящая из оболочки командной строки и связанного с ней языка сценариев.
Firewall	Системная утилита (сетевой экран) для контроля и фильтрации входящего/исходящего трафика.

VMware	Программное обеспечение виртуализации для облачных сред и центров обработки данных.
NetFlow	Сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems.
VPN	Виртуальная частная сеть — технология, которая позволяет установить безопасное подключение к сети Интернет.

### 3. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Раздел содержит описание функциональных возможностей Продукта.

Централизованная система аудита для предприятий любого размера. Обеспечивает эффективный сбор, обработку и хранение событий с поддерживаемых сервисов.

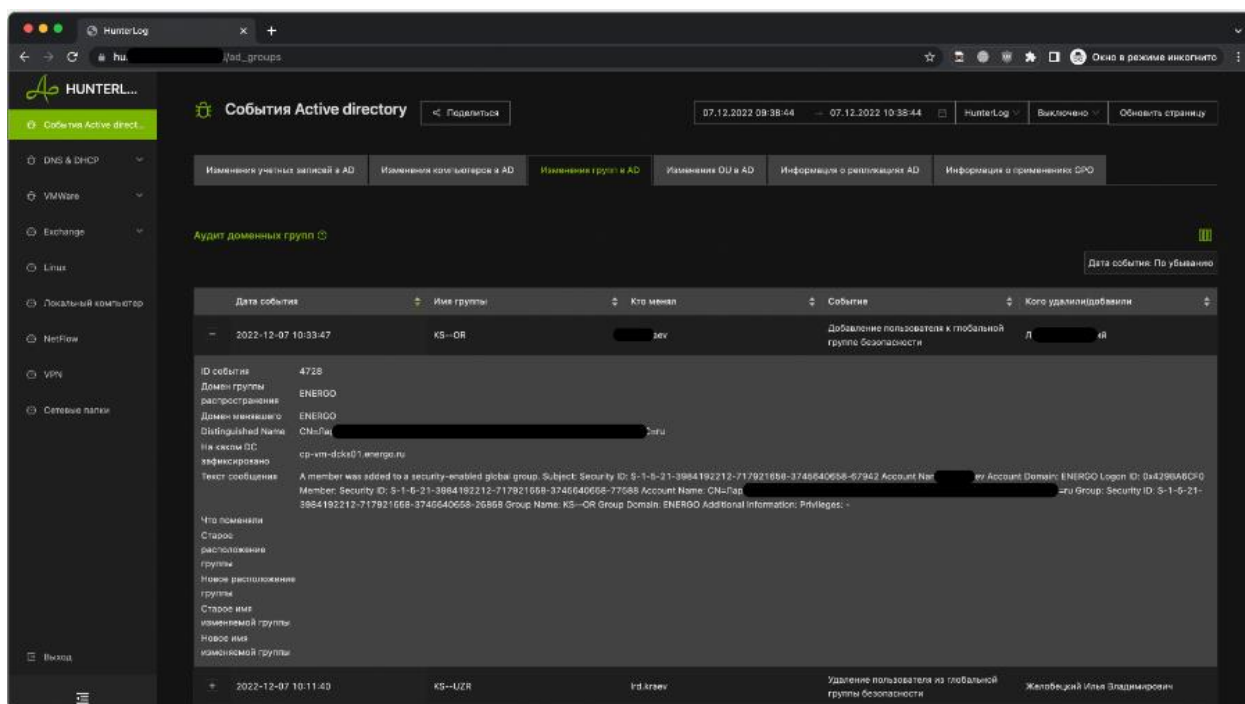
Идеология решения:

- Единая веб-консоль для всех отслеживаемых систем;
- Быстрый поиск с наглядным представлением событий;
- Расширенная детализация для поиска root cause причин возникновения сбоев;
- Высокоэффективное и экономичное хранение всех собранных данных;
- Построение цепочек из разных источников.

Отслеживание активности по следующим системам и сервисам:

#### Active Directory:

Раздел предназначен для получения информации о действиях с группами в AD.

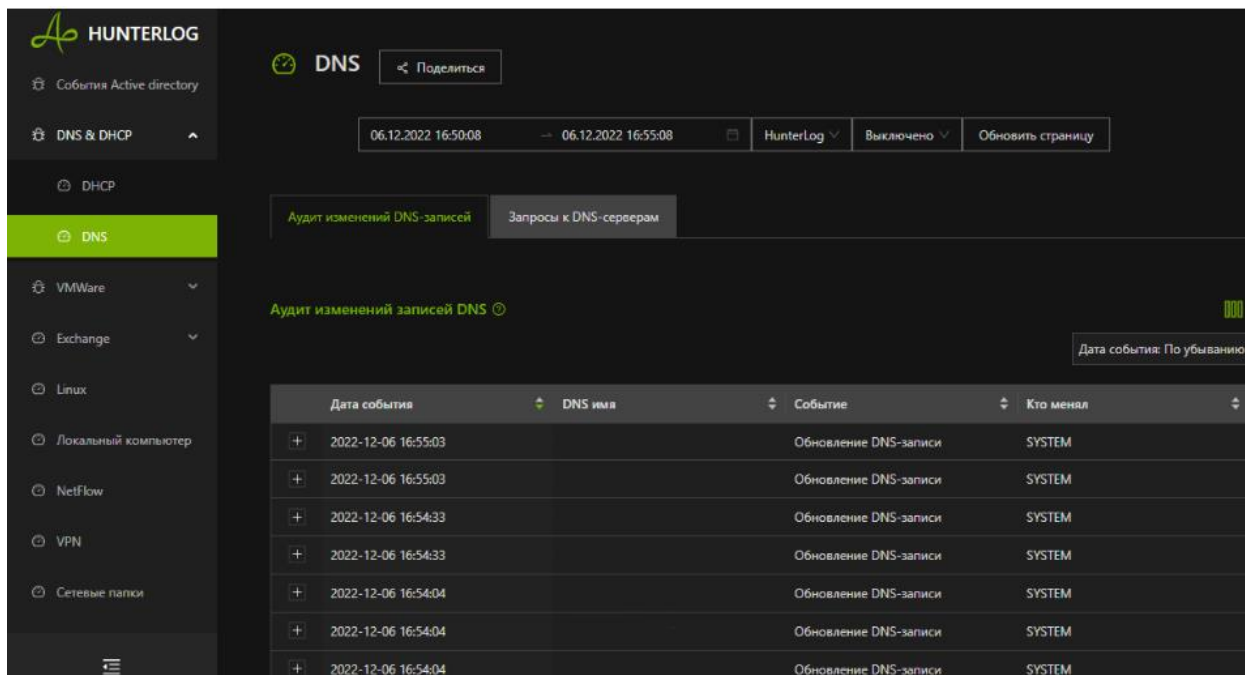


- Изменения групповых политик;
- Текущие права пользователей на назначение и применение политик;
- Отслеживание применения политик к объектам;
- Сохранение установленных и предыдущих значений после применения.

## Раздел DNS & DHCP

Раздел содержит события от служб разрешения имён и выдачи сетевых параметров. Правильная работа этих служб оказывает непосредственное влияние на работоспособность всей инфраструктуры: пользовательской и серверной. События покажут ошибки разрешения имён и проблемные устройства, оказывающие негативное воздействие в сети.

### DNS:

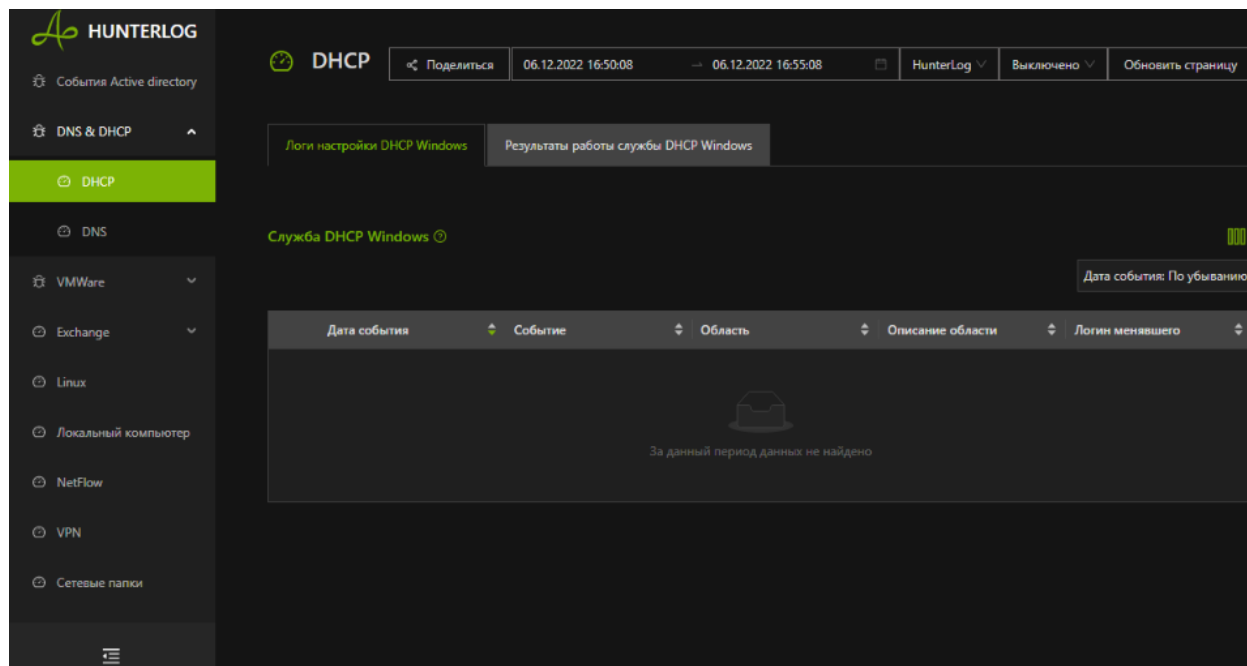


The screenshot displays the HUNTERLOG interface for DNS auditing. The main content area shows a table titled "Аудит изменений записей DNS" (DNS record change audit). The table has columns for "Дата события" (Event date), "DNS имя" (DNS name), "Событие" (Event), and "Кто менял" (Who changed). The events listed are all "Обновление DNS-записи" (DNS record update) performed by "SYSTEM" at various times on 2022-12-06.

Дата события	DNS имя	Событие	Кто менял
2022-12-06 16:55:03		Обновление DNS-записи	SYSTEM
2022-12-06 16:55:03		Обновление DNS-записи	SYSTEM
2022-12-06 16:54:33		Обновление DNS-записи	SYSTEM
2022-12-06 16:54:33		Обновление DNS-записи	SYSTEM
2022-12-06 16:54:04		Обновление DNS-записи	SYSTEM
2022-12-06 16:54:04		Обновление DNS-записи	SYSTEM
2022-12-06 16:54:04		Обновление DNS-записи	SYSTEM

- Изменения конфигурации и всех вносимых изменений;
- Добавление, удаление и изменение записей с сохранением значений;
- Ошибки обращения к службе разрешения имён;
- Поиск по событиям.

## DHCP:



- Изменения конфигурации серверов выдачи адресов;
- Отслеживание доступности служб;
- Мониторинг изменений в областях выдачи адресов;
- Оповещения о недостаточном количестве доступных адресов.

## Раздел Exchange:

В разделе представлены три категории событий: Мобильные клиенты - содержит события мобильных клиентов ActiveSync и веб-клиентов OWA. Системные события - внутренние события репликации DAG, баз внутри DAG, а также аудит запуска скриптов Powershell. Отслеживание писем Exchange - перечень принятых и отправленных писем с детализацией. События могут дублироваться.

Системные события Exchange

06.12.2022 16:50:08 → 06.12.2022 16:55:08

Репликация DAG Exchange | Репликация баз DAG Exchange | Аудит запуска скриптов Powershell

Репликация DAG

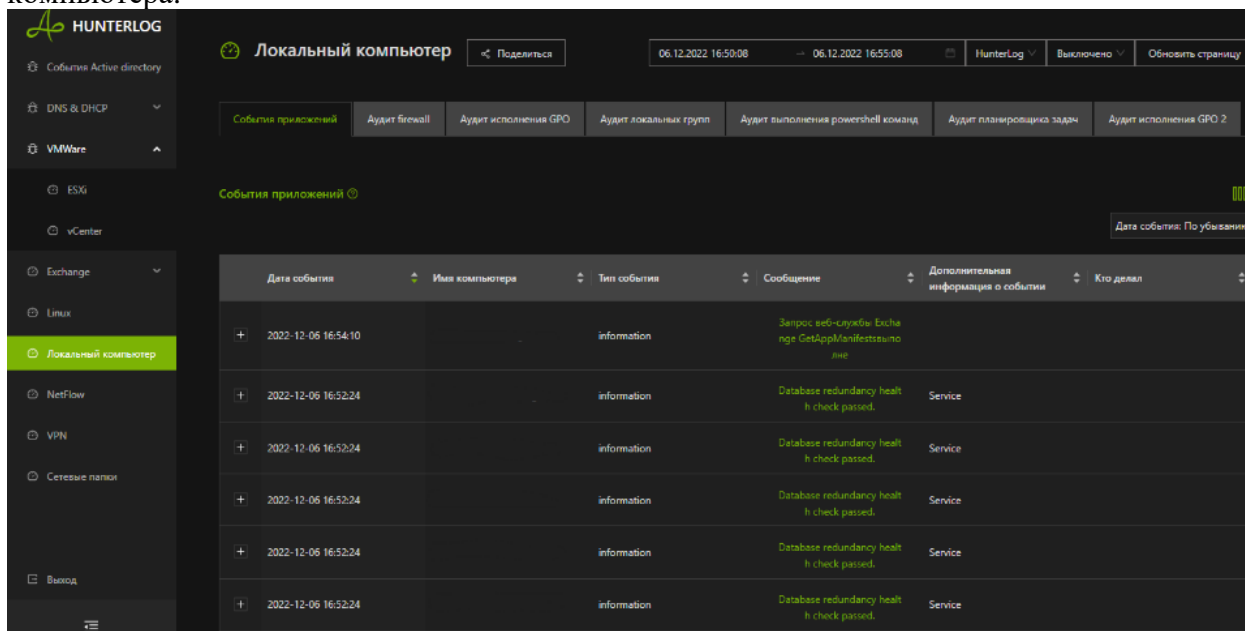
Дата события	Тип сообщения	Имя почтового сервера	Текст сообщения
2022-12-06 16:52:24	information		Database redundancy health check passed.
2022-12-06 16:52:24	information		Database redundancy health check passed.
2022-12-06 16:52:24	information		Database redundancy health check passed.
2022-12-06 16:52:24	information		Database redundancy health check passed.
2022-12-06 16:52:24	information		Database redundancy health check passed.

- Изменения конфигурации;
- Попытки доступа к привилегированным ящикам;
- Полная трассировка писем;
- Мониторинг доступности внешних адресов;
- Отслеживание возникновения аномалий (рост очередей, ошибки...);
- Отслеживание событий OWA и ActiveSync (мобильные клиенты);
- Состояние DAG (Database Available Group);
- Запуск PowerShell-скриптов;
- Загрузка/выгрузка почтовых ящиков.



## Раздел Локальный компьютер:

Ошибки и события, возникающие в рамках локальной операционной системы компьютера.



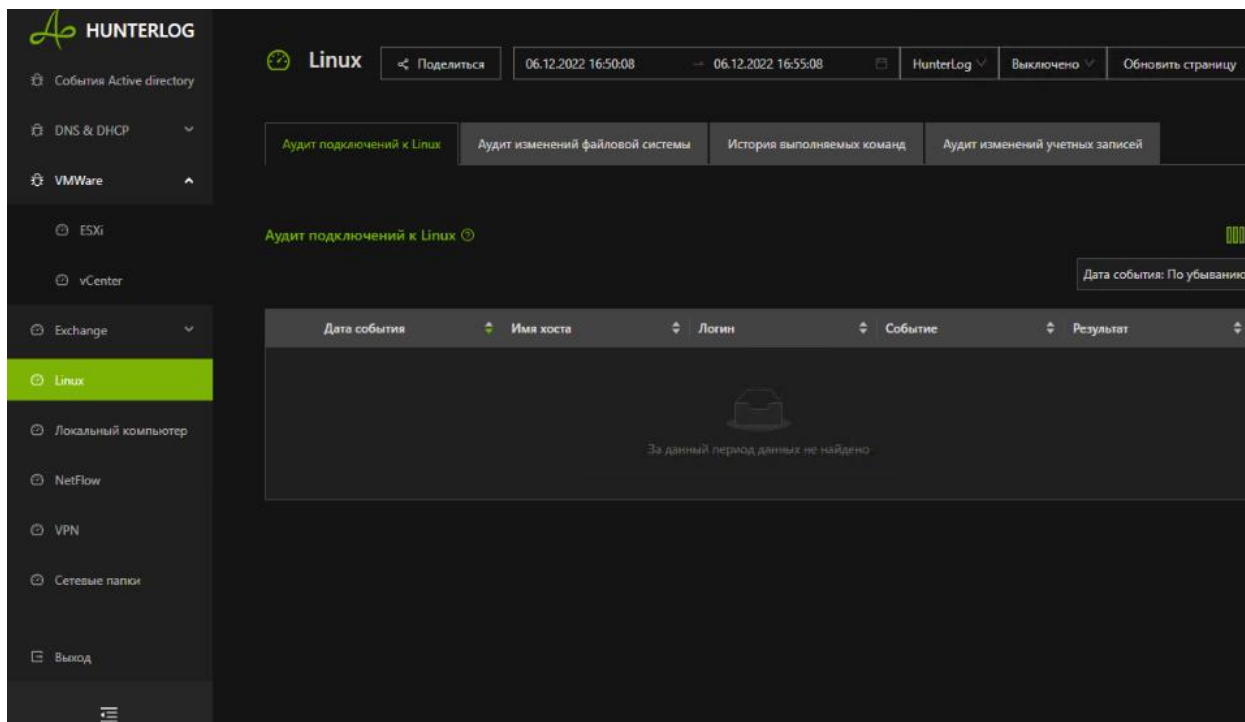
The screenshot shows the HUNTERLOG interface for the 'Локальный компьютер' (Local Computer) section. The left sidebar contains a navigation menu with items like 'События Active directory', 'DNS & DHCP', 'VMWare', 'ESX', 'vCenter', 'Exchange', 'Linux', 'Локальный компьютер' (highlighted), 'NetFlow', 'VPN', 'Сетевые папки', and 'Выход'. The main area shows a list of events under the heading 'События приложений'. The table below contains the following data:

Дата события	Имя компьютера	Тип события	Сообщение	Дополнительная информация о событии	Кто делал
2022-12-06 16:54:10		information	Запрос веб-службы: Exchange GetAppManifestы успешно		
2022-12-06 16:52:24		information	Database redundancy health check passed.	Service	
2022-12-06 16:52:24		information	Database redundancy health check passed.	Service	
2022-12-06 16:52:24		information	Database redundancy health check passed.	Service	
2022-12-06 16:52:24		information	Database redundancy health check passed.	Service	
2022-12-06 16:52:24		information	Database redundancy health check passed.	Service	

- Изменение локальных групп и учетных записей;
- Применение GPO;
- Изменения в планировщика заданий;
- Изменения в firewall-е.

## Раздел Linux:

События, связанные с операционной деятельностью системы Linux.



The screenshot shows the HUNTERLOG interface for the 'Linux' section. The left sidebar contains a navigation menu with items like 'События Active directory', 'DNS & DHCP', 'VMWare', 'ESX', 'vCenter', 'Exchange', 'Linux' (highlighted), 'Локальный компьютер', 'NetFlow', 'VPN', 'Сетевые папки', and 'Выход'. The main area shows a list of events under the heading 'Аудит подключений к Linux'. The table below contains the following data:

Дата события	Имя хоста	Логин	Событие	Результат
За данный период данных не найдено				

- Изменение файлов;

- Изменения учетных записей и групп;
- Входы/выходы;
- Логи вводимых команд.

## Раздел VMware

- Сбор событий как с локальных хостов, так и с vcenter;
- Создание/изменение/удаление объектов;
- Работа внутренних служб (DRM, scheduler);
- Входы/выходы как для локальных хостов, так и для vcenter.

В разделе представлены две категории событий: ESXi - содержит события от хостов виртуализации vCenter - события от сервера управления инфраструктурой виртуализации. События могут дублироваться.

### ESXi

При переходе открывается страница аудита событий хостов виртуализации

The screenshot shows the HUNTERLOG interface for ESXi events. The main content area displays the following table:

Дата события	Имя сервера esxi	Тип сообщения	Кто делал	Имя VM	Действие
2022-12-06 16:50:27		info			Removed

## vCenter

При переходе открывается страница сообщений об ошибках сервера управления

The screenshot shows the vCenter monitoring interface. The left sidebar contains navigation options: События Active directory, DNS & DHCP, VMWare, ESX, vCenter (highlighted), Exchange, Linux, Локальный компьютер, NetFlow, VPN, and Сетевые папки. The main area displays a table of vCenter error messages. The table has columns for Date, Name, Type, Who did it, Date range, Name of the event, Description of the change, and Area. The messages are:

Дата события	Имя vcenter	Тип сообщения	Кто делал	Имя дататора	Название предупреждения	Описание изменения статуса	Имя области
2022-12-06 16:54:28		info			Убрана HA virtual machine fallback failed	changed from Gray to Green	
2022-12-06 16:51:33		info			Virtual machine CPU usage	changed from Gray to Green	
2022-12-06 16:51:33		info			Virtual machine memory usage	changed from Gray to Green	
2022-12-06 16:50:53		info			Virtual machine CPU usage	changed from Yellow to Green	

## Раздел NetFlow

События сетевого взаимодействия и потоков данных протокола NetFlow.

При переходе открывается страница соединений и переданных данных с детализацией:

The screenshot shows the NetFlow monitoring interface. The left sidebar contains navigation options: События Active directory, DNS & DHCP, VMWare, Exchange, Мобильные клиен..., Системные событ..., Отслеживание пи..., Linux, Локальный компьютер, NetFlow (highlighted), VPN, and Сетевые папки. The main area displays a table of NetFlow data transfer details. The table has columns for Data transferred, Source IP, Source Port, Dest IP, Dest Port, Protocol, and Quantity. The data is:

Передано данных	Source IP	Source Port	Dest IP	Dest Port	Протокол	Количество
287.48 MB		63632		HTTPS (443)	TCP	4
220.78 MB		Oracle (1521)		63061	TCP	4
113.11 MB		45102		Elasticsearch binary (9300)	TCP	5
110.78 MB		45078		Elasticsearch binary (9300)	TCP	10
75.11 MB		SMB без NetBios (445)		9695	TCP	7
44.66 MB		34796		Elasticsearch binary (9300)	TCP	2

## Раздел VPN

События удалённого подключения пользователей.

- Cisco

- OpenVPN
- Wireguard

При переходе открывается страница Cisco AnyConnect VPN с детализацией установления подключений:

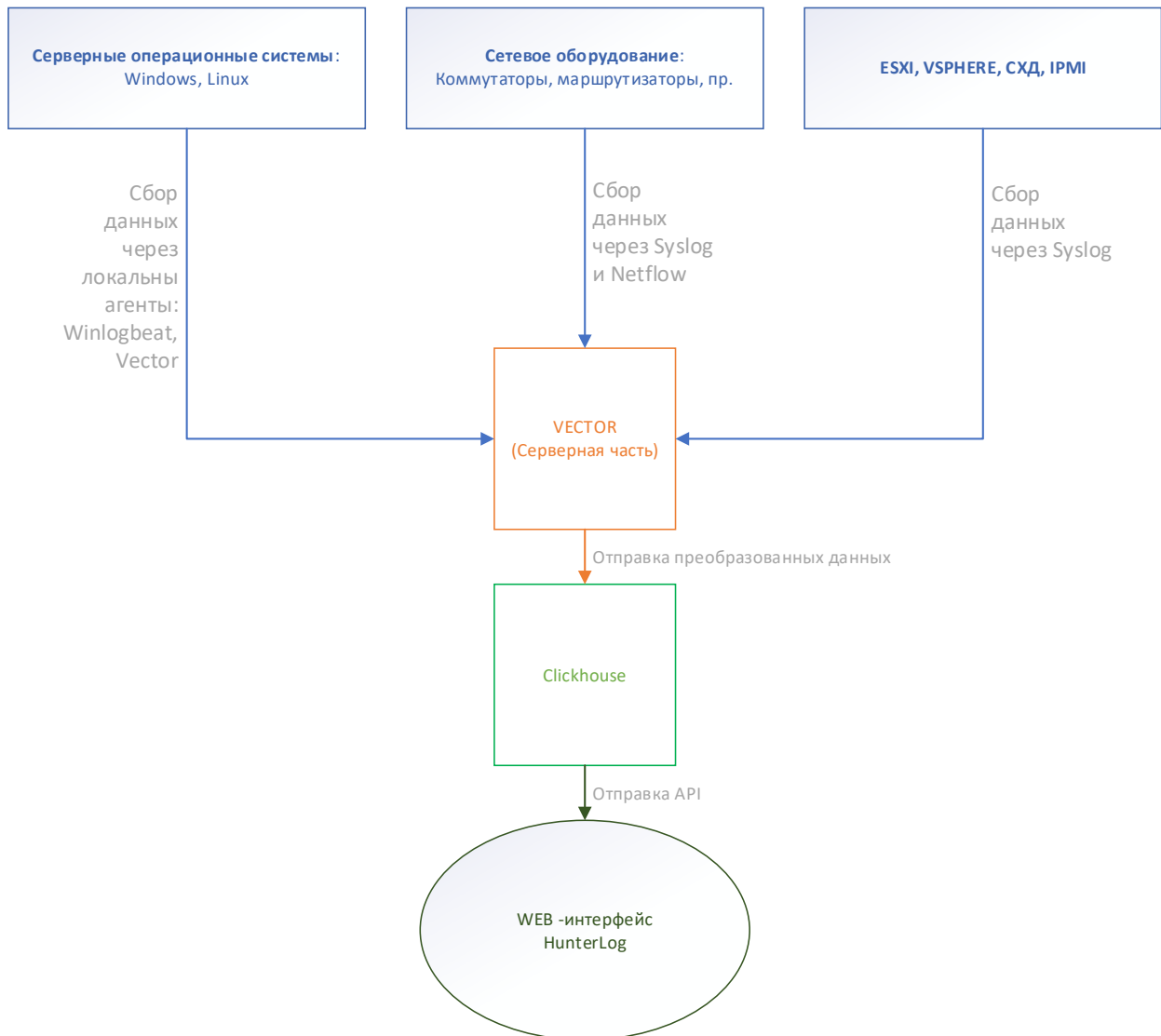
The screenshot shows the HUNTERLOG interface for monitoring VPN connections. The left sidebar contains a navigation menu with categories like 'События Active directory', 'DNS & DHCP', 'VMWare', 'Exchange', and 'VPN' (highlighted). The main area displays 'Cisco AnyConnect VPN' with a search filter 'VPN' and a 'Поделиться' button. A date range filter is set to '06.12.2022 16:50:08' to '06.12.2022 16:55:08'. Below this, there's a section for 'Cisco VPN' with a table of events.

Время события	Имя или IP-адрес устройства	ID события	Имя пользователя	Внешний IP-адрес подключающегося клиента	Подробности по событию	Группа VPN, к которой относится пользователь
2022-12-06T13:55:08		002			Процесс SSL handshake с удалённым устройством завершился успешно	
2022-12-06T13:55:08		005			Сервер запросил сертификат Secure Firewall ASA для аутентификации	Идентифициров

Поиск по любым событиям не является конечным, все полученные данные могут быть отсортированы и отфильтрованы в соответствии с задачей.

#### 4. АРХИТЕКТУРА

При разработке и эксплуатации Продукта используется следующий стек технологий:



## **5. ЮРИДИЧЕСКАЯ ИНФОРМАЦИЯ**

### **Авторские права**

Материалы, приведенные в настоящем документе, являются собственностью ООО «Дигилабс» и могут быть использованы только специалистами для целей экспертной проверки Системы в рамках процедуры включения в Единый реестр российских программ для электронных вычислительных машин и баз данных, а также для личных целей приобретателей программного обеспечения.

Запрещается воспроизведение отдельных частей документа, внесение правок в него, размещение на сетевых ресурсах, распространение в любой форме (в том числе в переводе) на бумажных и электронных носителях, посредством каналов связи и средств массовой информации или каким-либо другим способом без специального письменного разрешения ООО «Дигилабс» и ссылки на источник.

Программное обеспечение и товарные знаки, указанные в настоящем документе, принадлежат ООО «Дигилабс» и охраняются законом.

### **Содержание документа**

Содержание данного документа может изменяться без предварительного уведомления. ООО «Дигилабс» не несёт ответственности за неточности и/или ошибки, допущенные в данном документе, и возможный ущерб, связанный с этим.