ООО Дигилабс
ОГРН: 1207700443532, ИНН: 7707445960, КПП: 770701001

Программный продукт **ХантерЛог (HunterLog)**

Документация, содержащая информацию, необходимую для эксплуатации экземпляра программного обеспечения, предоставленного для проведения экспертной оценки в Экспертном совете при Минцифры России

Москва
2022 г.

Оглавление

1. ОПИСАНИЕ СИСТЕМЫ, ВХОД НА ПОРТАЛ

Система ХантерЛог - централизованная система аудита для предприятий любого размера. Обеспечивает эффективный сбор, обработку и хранение событий с поддерживаемых сервисов. Отслеживание и своевременная реакция на соответствующие сообщения могут предсказать и предотвратить сбои, ошибки, низкую скорость работы и возможные атаки злоумышленников на ключевые корпоративные информационные системы.

Доступ к системе осуществляется через веб-интерфейс при помощи любого из поддерживаемых браузеров. У портала простая и интуитивно понятная навигация. Вход осуществляется через логин и пароль, выданный ранее.

2. ОБЩИЙ ВИД ПОРТАЛА

После аутентификации на портале открывается окно «События Active directory». Внешний вид представлен на рисунке 1.

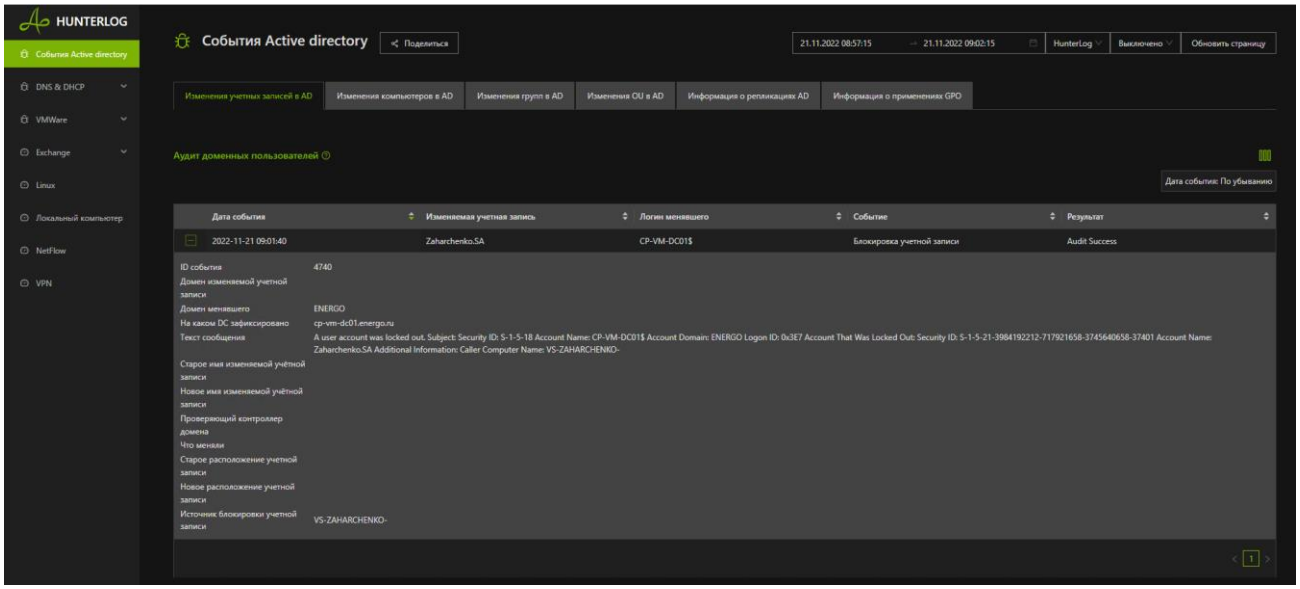

Рис.1 (общий вид портала)

Доступны следующие элементы навигации по порталу:

- Меню слева — перемещение в любой интересующий раздел;
- Выбор диапазона в верхнем правом углу — возможность конкретизации условий поиска с указанием временного диапазона и выбором нужного сервиса с автообновлением результатов;
- Команда «Поделиться» - возможность скопировать ссылку на конкретную выборку событий.

Далее в документе приводится детальная информация по каждому разделу портала, а также типовые сценарии работы в реальной инфраструктуре.

3. ОСНОВНЫЕ РАЗДЕЛЫ И НАЗНАЧЕНИЕ

В данном разделе приведено детальное описание всех экранов портала.

События Active directory

Экран представляет собой агрегированную информацию по следующим метрикам:

- Изменение учетных записей в AD;
- Изменения OU/CN;

- Изменения в группах;
- Изменения компьютеров;
- Репликация AD.

Информация выводится за выбранный период времени и для выбранного сервиса. Для автоматического обновления данных можно выставить период в секундах.

Внешний вид экрана «**Изменение учетных записей в AD**» представлен на рисунке 2. Показаны учетные записи, логин менявшего, событие, результат. При детализации строки представлена дополнительная информация по домену, тексту сообщения и т.п.

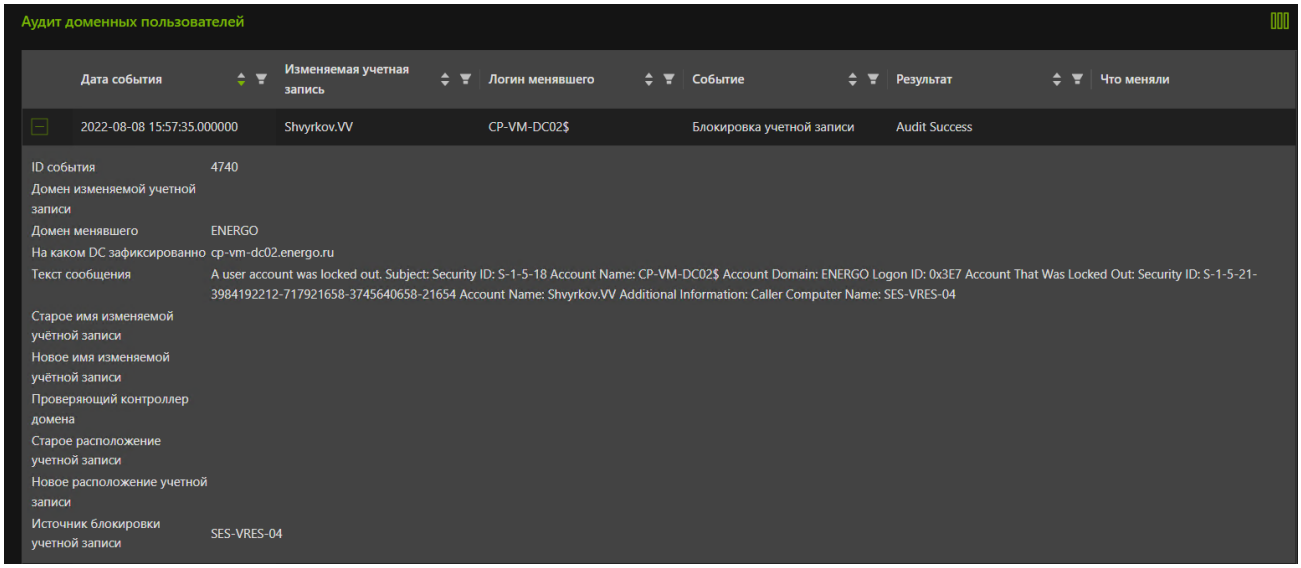

Рис. 2

На следующей вкладке «**Изменения OU/CN**» (рис.3) отображается информация об изменении подразделений и групп в Active directory. Доступна детализация каждой строки, с указанием логина менявшего, старое и новое расположение, старое и новое имя, а также событие.

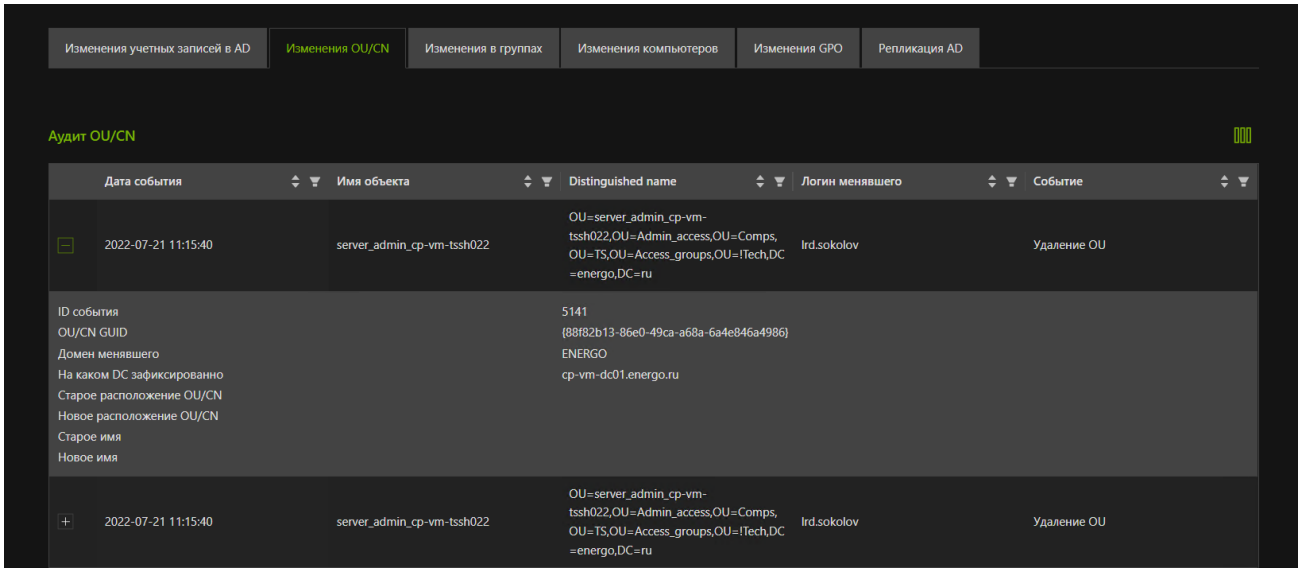

Рис. 3

На вкладке «**Изменения в группах**» (рис.4) отображаются данные по изменению доменных групп в разрезе имени группы, изменяющего пользователя, события, добавленного/удаленного в группу. При детализации строки отображается дополнительная развернутая информация, включающая текст сообщения, на каком DC зафиксировано изменение, и детальная информация по изменению.

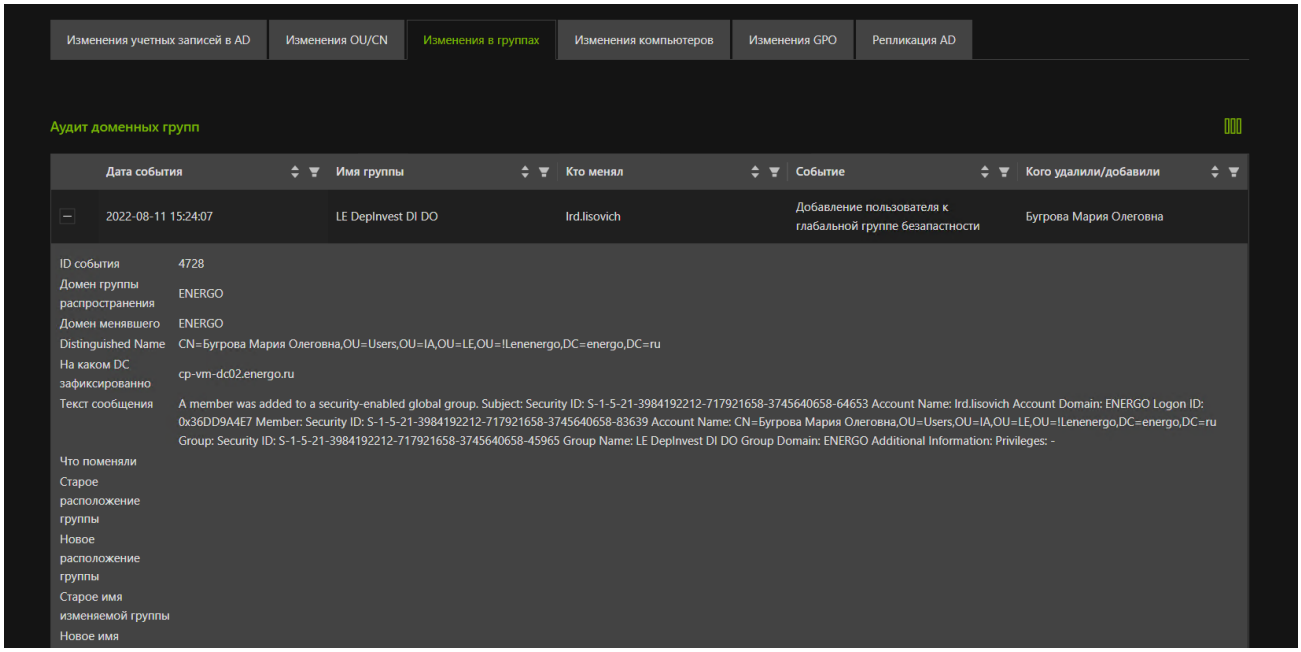

Рис. 4

На следующей вкладке «**Изменения компьютеров**» (рис.5) представлена информация об изменении данных, включающих такие события как: изменение учетных записей компьютера, добавление компьютера в домен, удаление компьютера из домена, перемещение учетной записи компьютера по структуре AD, переименование компьютера. Детализация строки содержит данные по старым/новым именам, результат события, текст сообщения.

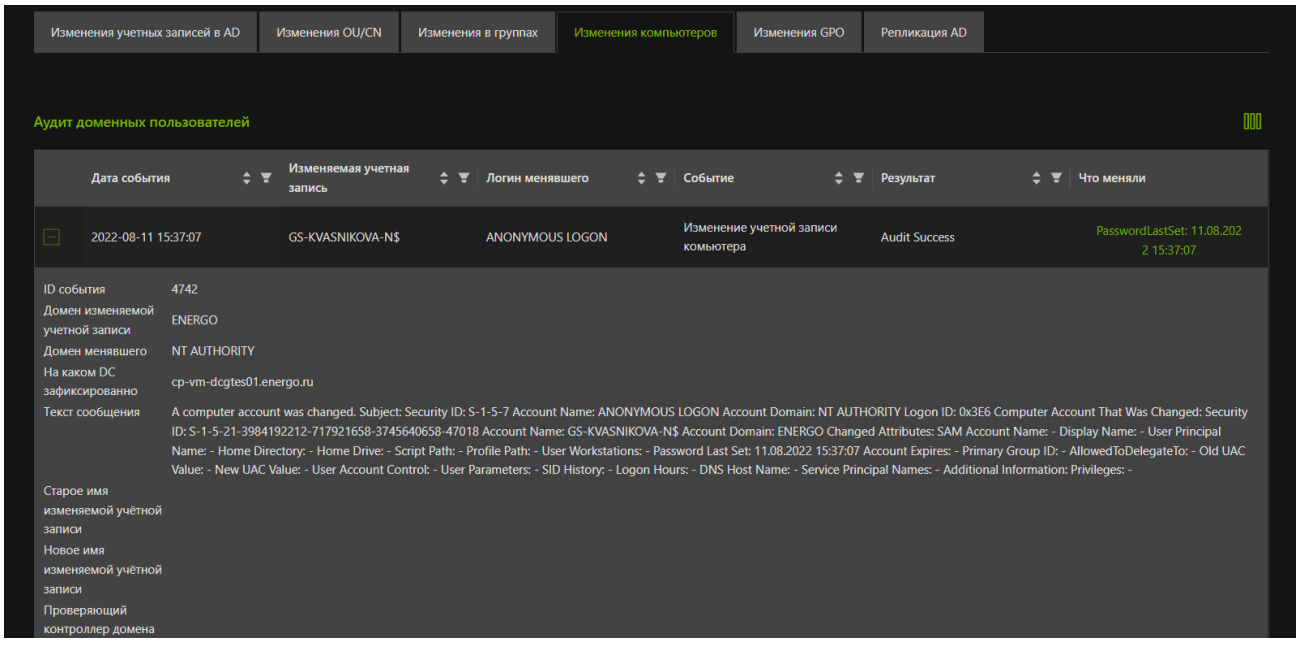

Рис. 5

Вкладка «Репликация AD» (рис.6) отображает информацию о проблемах в AD с описанием случившегося, включая тип сообщения, его текст и DC, где событие было зафиксировано.

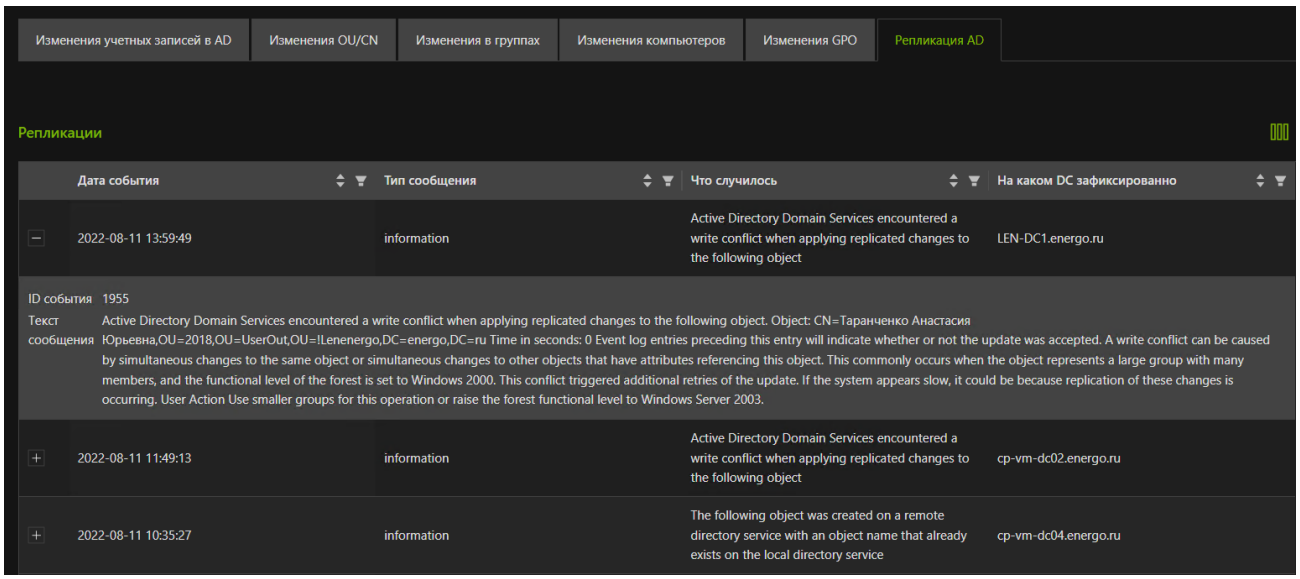

Рис. 6

На всех вкладках в таблицах доступен отбор и сортировка записей каждой колонки для удобства сбора данных.

DNS & DHCP

Раздел «DNS & DHCP» раздел на два подраздела – DNS и DHCP, где выведена детальная информация по событиям, а также реализован удобный поиск по логам.
DHCP:
На рисунке 7 представлена таблица с логами настроек DHCP Windows, где за выбранный период выводятся события в разрезе даты, описания области, логов менявшего, самого изменения, старых и новых значениях, ip-адреса и имя DHCP- сервера.

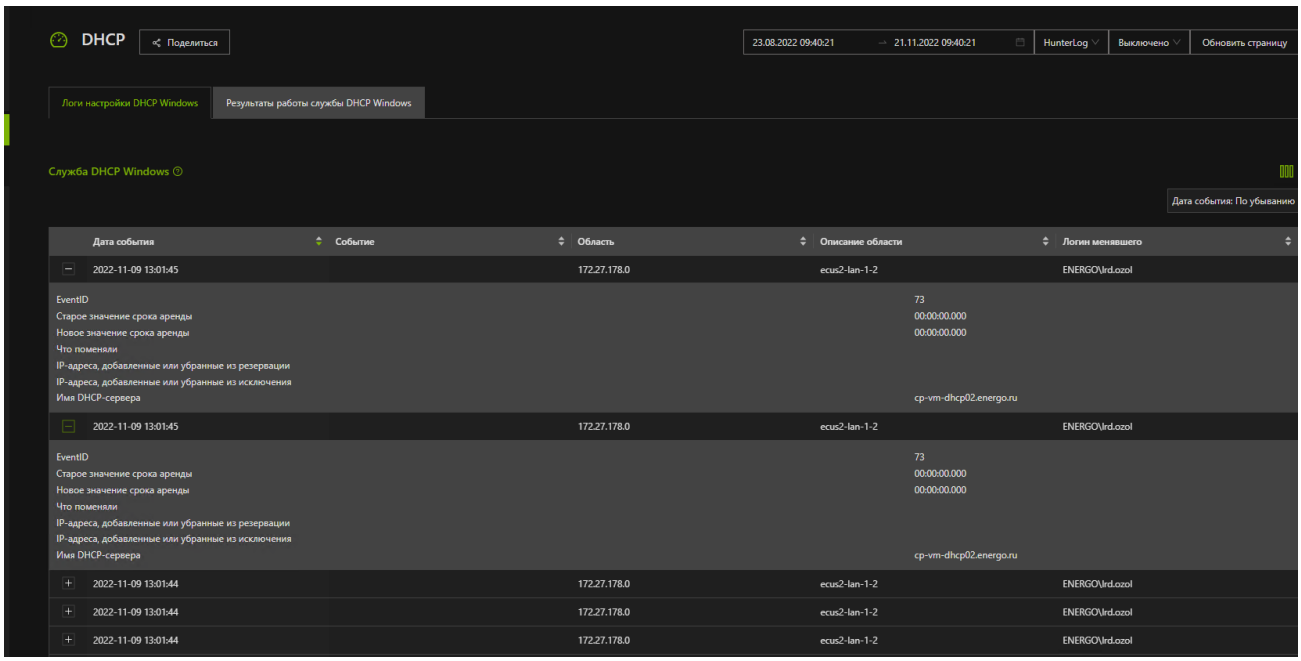

Рис. 7

На следующей вкладке «Результаты работы службы DHCP Windows» (рис.8) отображается таблица, включающая следующие данные:

- Имя DHCP-сервера;
- Действие;
- Выданный/обновленный IP;

- Имя хоста клиента;

- MAC-адрес хоста-клиента.

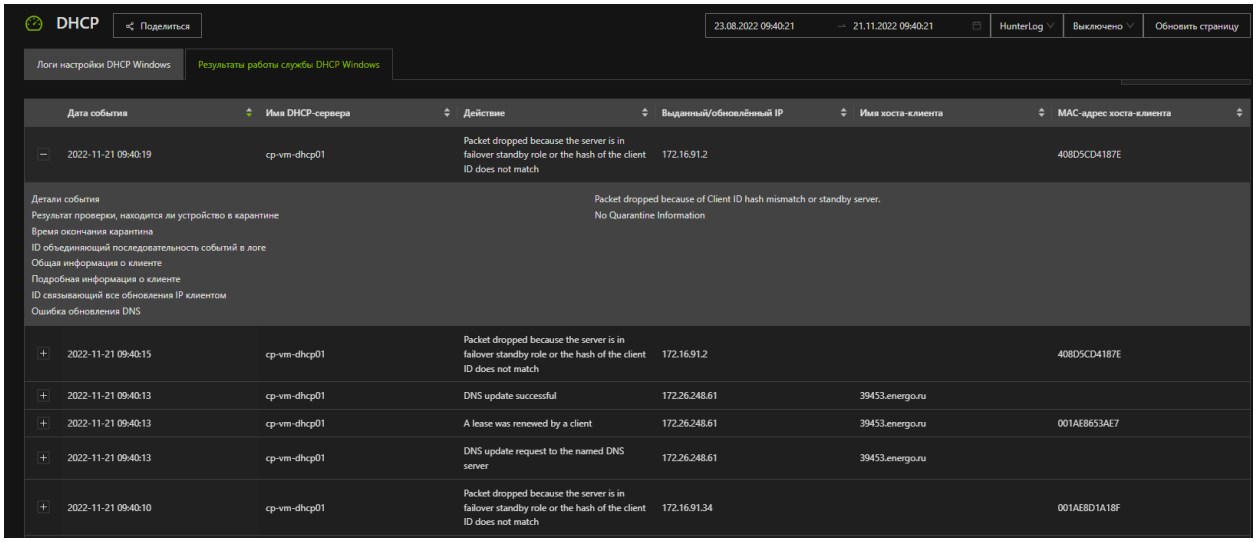

Рис.8

DNS:
В подменю расположено две вкладке: «Аудит изменений DNS-записей» и «Запросы к DNS-серверам».

Аудит изменений DNS-записей (рис.9)
За выбранный период отображается информация о дате события, DNS-имени, события, а также инициатора – кто менял.

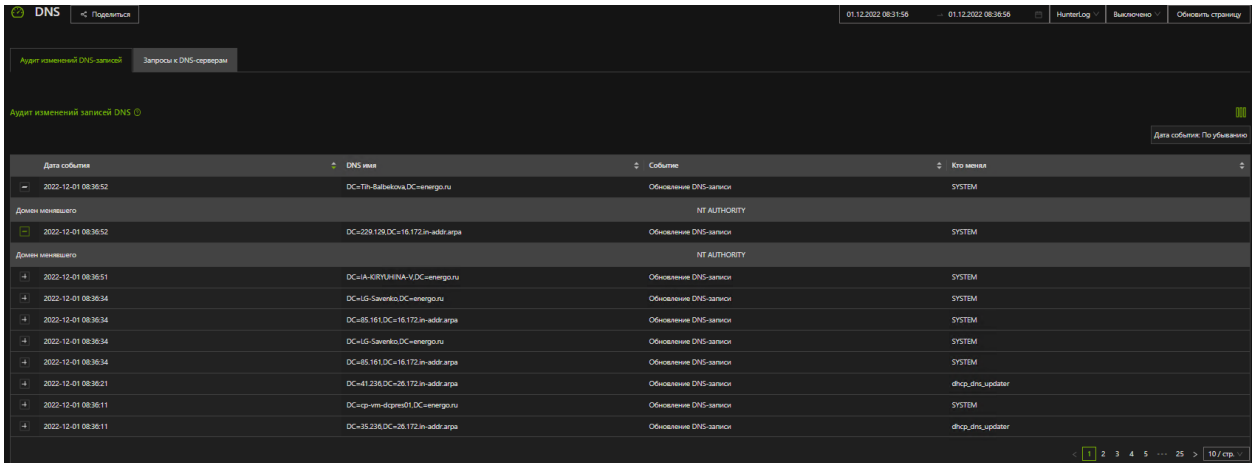

Рис. 9

Запросы к DNS-серверам (рис.10)

Отображение информации в разрезе:
- Дата события;
- Имя DNS-сервера;
- Событие;
- Тип запроса;
- Запрашиваемое DNS-имя;
- Тип запрашиваемого имени;
- IP-адрес делавшего запрос.

По всем столбцам доступна сортировка данных.

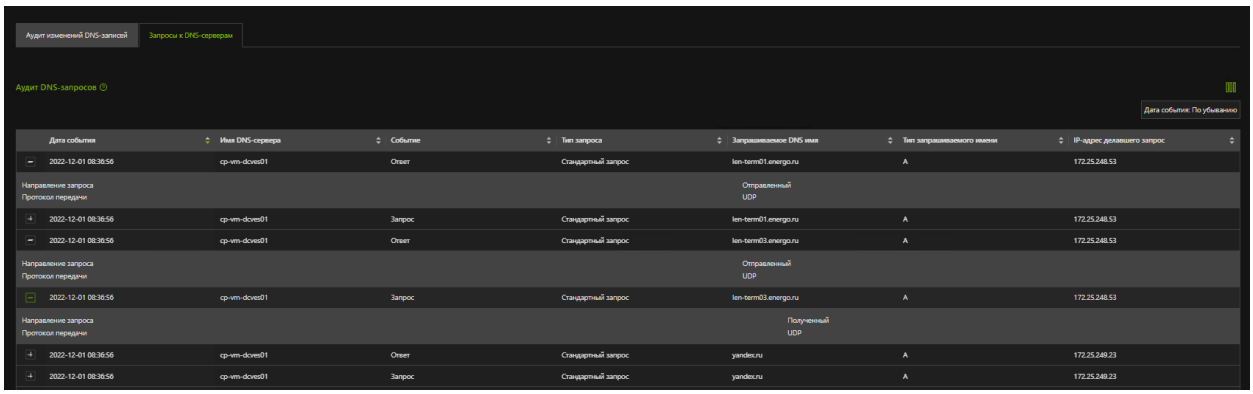

Рис.10

VMWare:

Раздел «VMWare» состоит из двух подразделов «ESXi» и «vCenter», в которых представлена общая аналитика по виртуализации, ошибкам, аудиту.

«ESXi»

Данный подраздел представлен в виде следующих вкладок:

- **Аудит событий ESXi** (рис.11):

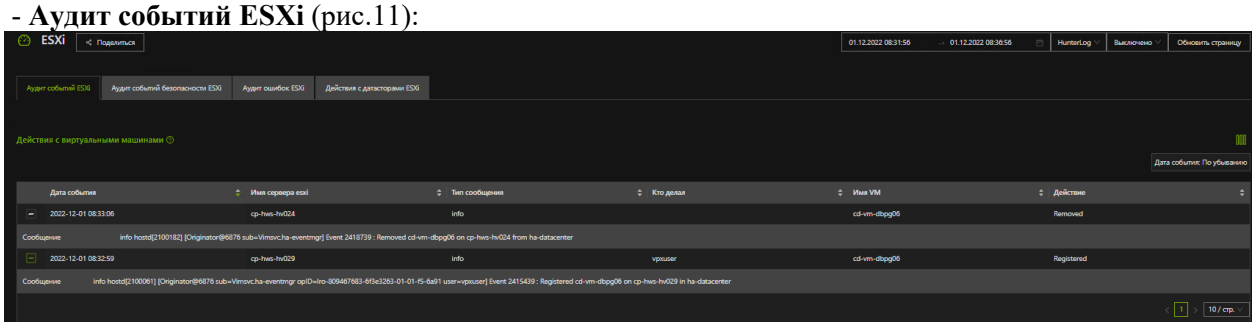

Рис.11

Пользователю доступны следующие данные:
- Дата события;
- Имя сервера ESXi;
- Тип сообщения;
- Кто делал;
- Имя VM;
- Действие.

При детализации каждой строки доступно сообщение.

- **Аудит событий безопасности ESXi** (рис.12):

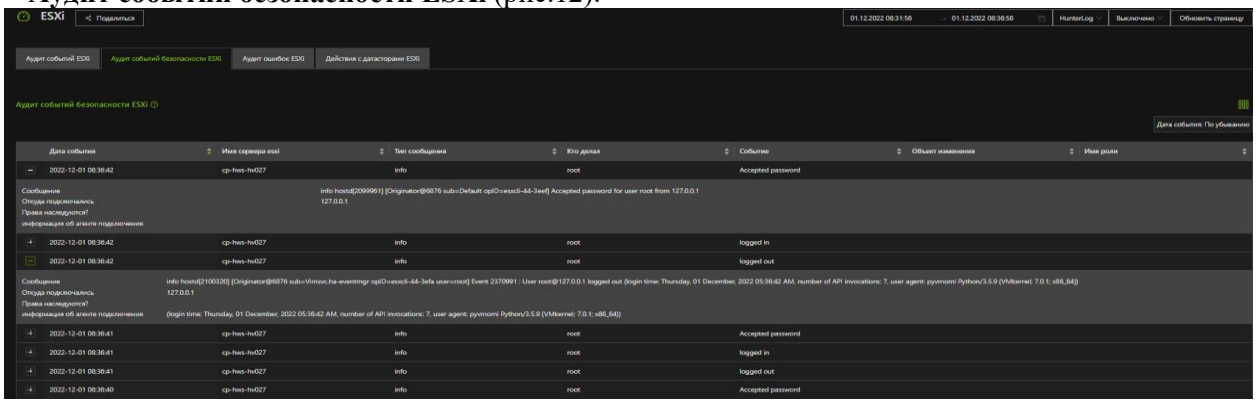

Рис.12

На странице представлена информация в разрезе:
- Дата события;
- Имя сервера ESXi;
- Тип сообщения;
- Кто делал;
- Событие;
- Объект изменения;
- Имя роли.

При детализации каждой строки пользователю доступны следующие данные:
- Сообщение;
- Откуда подключались;
- Права наследуются?
- Информация об агенте подключения.

- **Аудит ошибок ESXi** (рис.13):

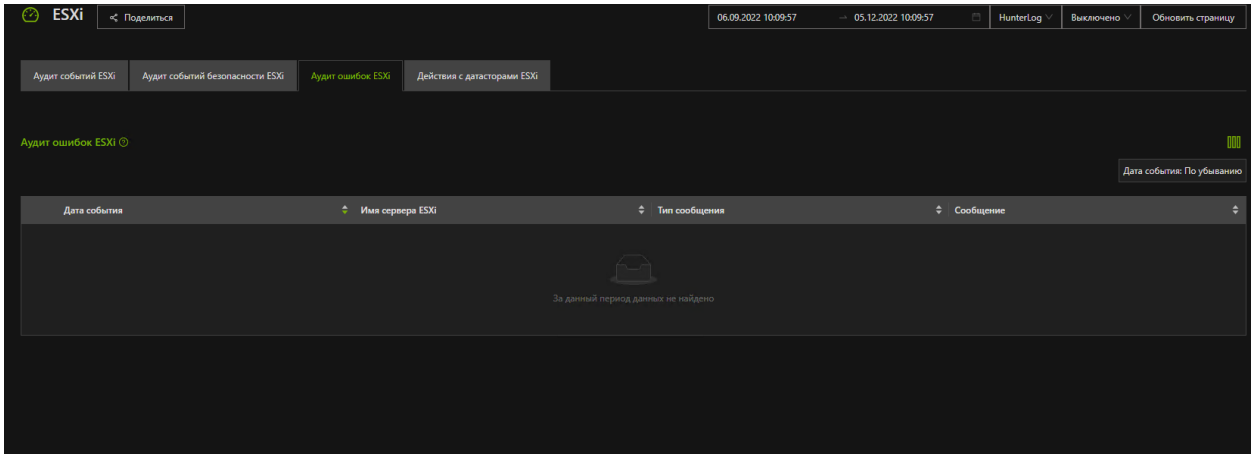

Рис.13

Аудит ошибок предоставляет информацию в разрезе:
- Дата события;
- Имя сервера ESXi;
- Тип сообщения;
- Сообщение.

За выбранный в примере период ошибок не обнаружено.
- **Действия с датасторами ESXi** (рис.14):

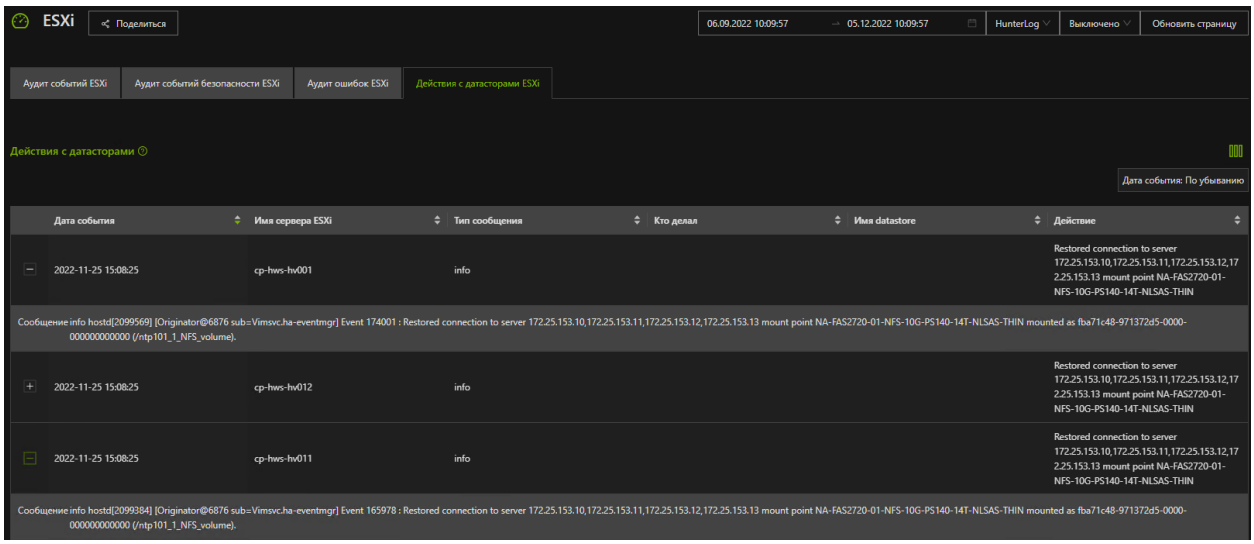

Рис.14

На данной вкладке представлена информация по действиям с датасторами в разрезе следующих полей:
- Дата события;
- Имя сервера ESXi;
- Тип сообщения;
- Кто делал;
- Имя datastore;
- Действие.

При детализации строки есть возможность получить информацию о сообщении по этому событию.

«vCenter»

Данный подраздел представлен в виде следующих вкладок:

- **Сообщения об ошибках vCenter** (рис.15):

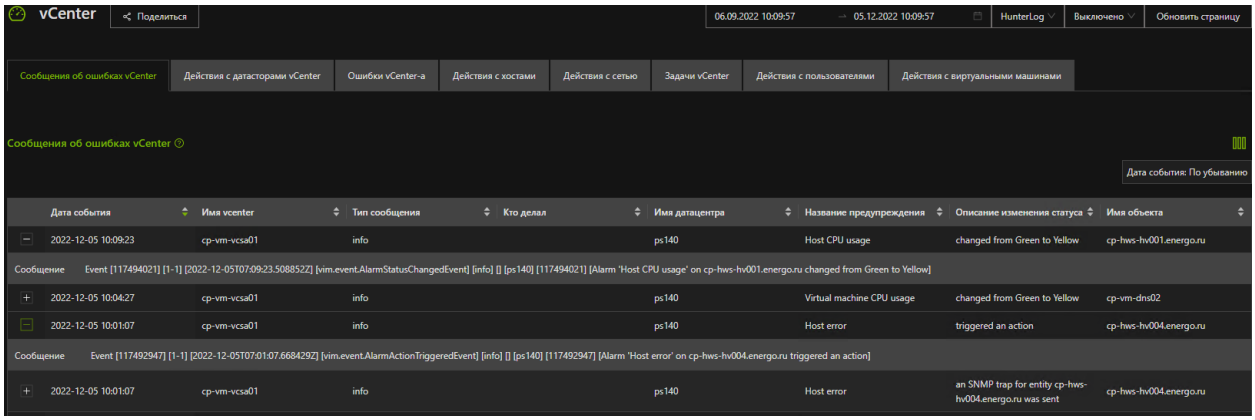

Рис.15

На данной странице подробно представлена информация по ошибкам в виде следующих данных:
- Дата события;
- Имя vcenter;
- Тип сообщения;
- Кто делал;
- Имя датацентра;
- Название предупреждения;
- Описание изменения статуса;
- Имя объекта.

При детализации строки есть возможность получить информацию о сообщении по этому событию.

- **Действия с датасторами vCenter** (рис.16):

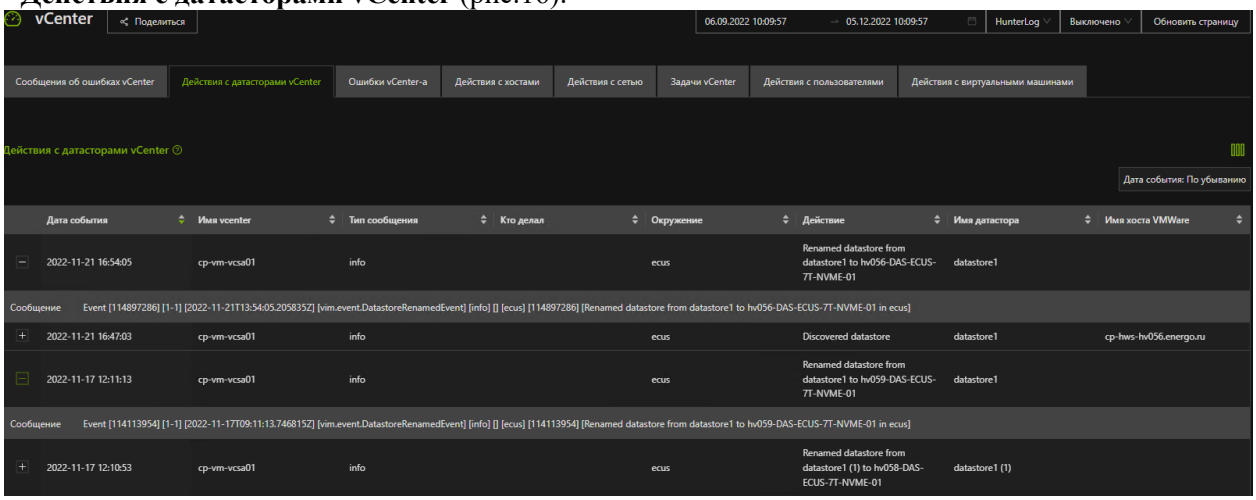

Рис.16

На странице представлены следующие данные:
- Дата события;
- Имя vCenter;
- Тип сообщения;
- Кто делал;
- Окружение;
- Действие;
- Имя датастора;
- Имя хоста VMWare.

По каждой строке выводится информация в виде сообщения. Пользователю доступна сортировка по каждой представленной колонке.

- **Ошибки vCenter-a** (рис.17):

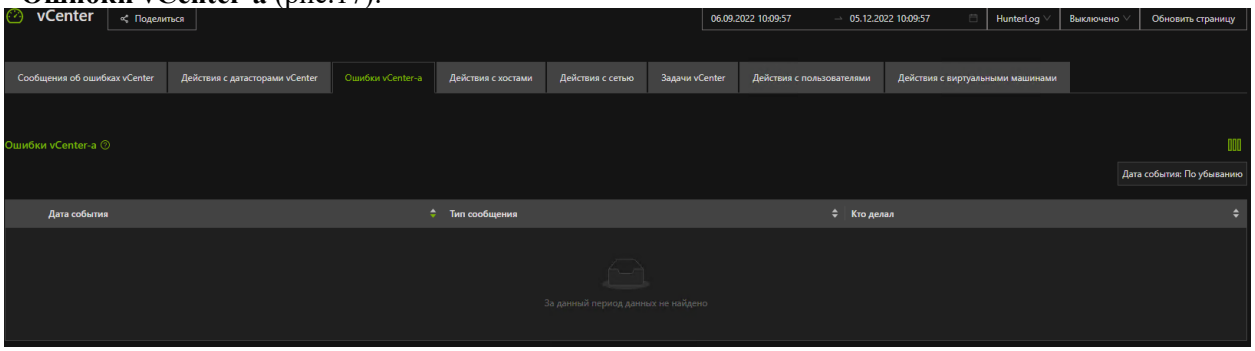

Рис.17

Все выявленные ошибки за указанный период отображаются на странице в разрезе:
- Дата события;
- Тип сообщения;
- Кто делал.

На рисунке отстутсвует информация, так как за выбранный период ошибок не обнаружено.

- **Действия с хостами** (рис.18):

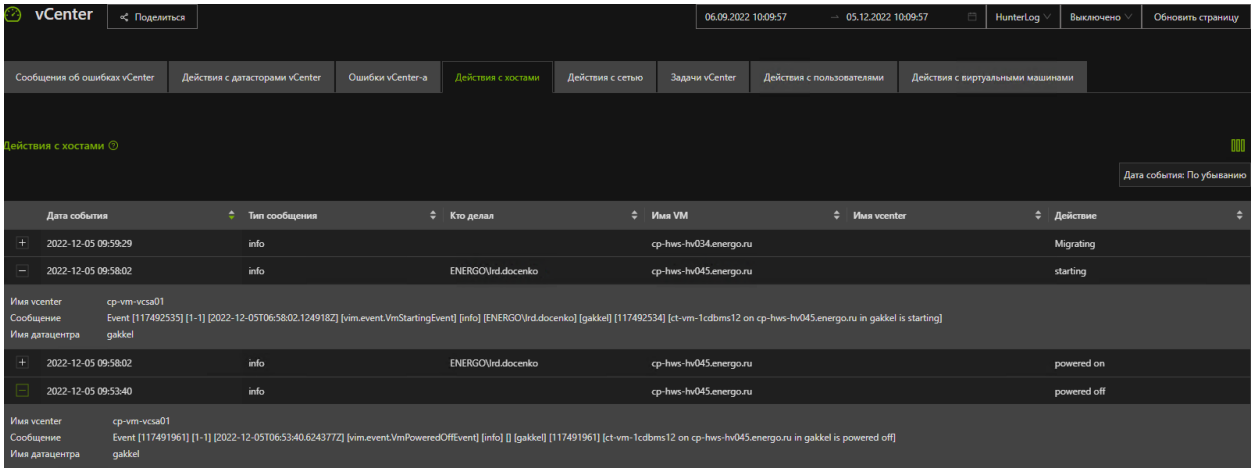

Рис.18

На текущей вкладке пользователю представлена детальная, подробная информация по событиям действий с хостами в разрезе:
- Дата события;
- Тип сообщения;
- Кто делал;
- Имя VM;
- Имя vcenter;
- Действие.

При детализации строки выводится информация, содержащая:
- Имя vcenter;
- Сообщение;
- Имя датацентра.

По всем колонкам доступна сортировка данных для удобства пользования.

- **Действия с сетью** (рис.19):

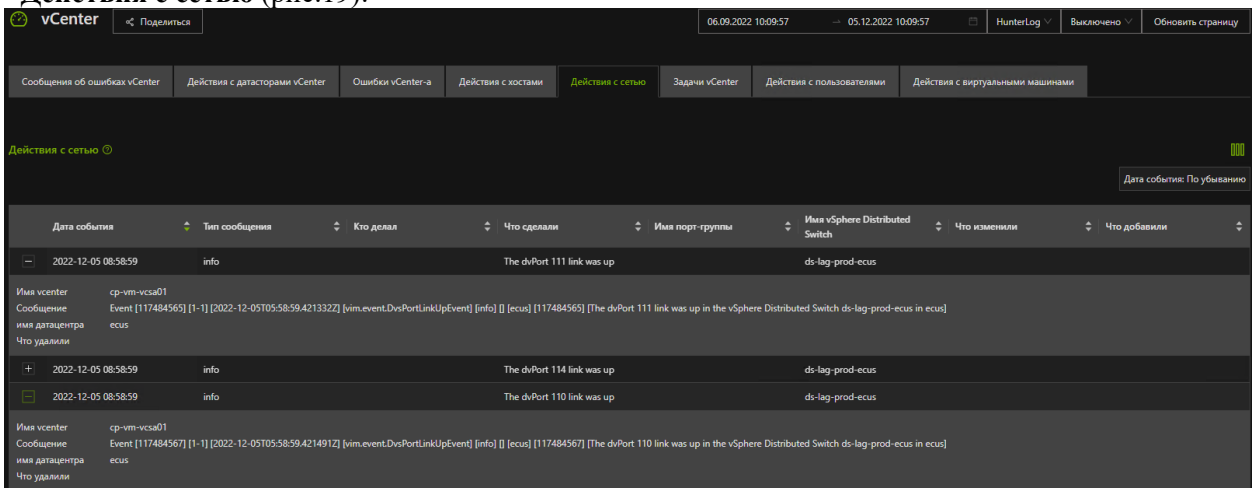

Рис.19

На вкладке отображаются все действия с сетью за выбранный период. Вся информация сгруппирована по следующим полям:
- Дата события;
- Тип сообщения;
- Кто делал;
- Что сделано;
- Имя порт-группы;
- Имя vSphere Distributed Switch;

- Что изменили;
- Что добавили.

При детализации строки выводится дополнительная информация:
- Имя vcenter;
- Сообщение;
- Имя датацентра;
- Что удалили.

По всем колонкам доступна сортировка данных для удобства пользования.

- **Задачи vCenter** (рис.20):

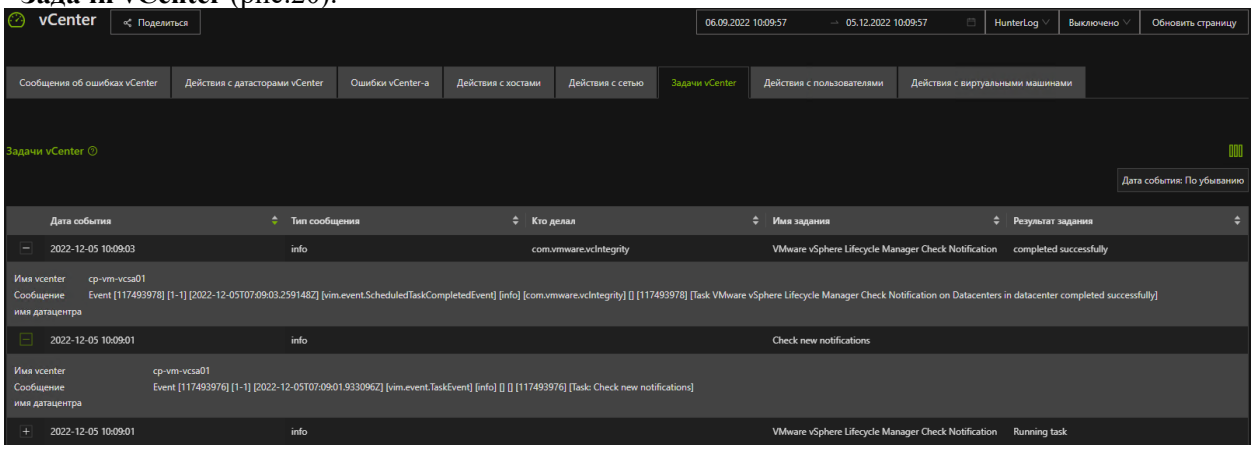

Рис.20

На вкладке отображаются все задачи за выбранный период. Вся информация сгруппирована по следующим полям:
- Дата события;
- Тип сообщения;
- Кто делал;
- Имя задания;
- Результат задания.

При детализации строки выводится дополнительная информация:
- Имя vcenter;
- Сообщение;
- Имя датацентра.

По всем колонкам доступна сортировка данных для удобства пользования.

- **Действия с пользователями** (рис.21):

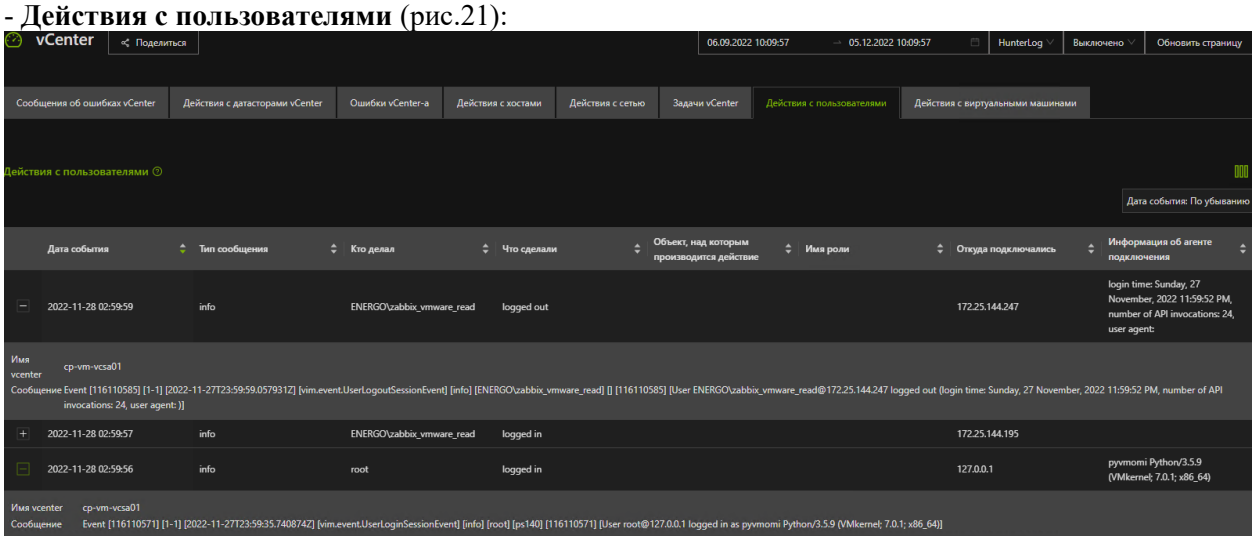

Рис.21

На странице действий с пользователями представлены данные за выбранный период с группировкой по следующим полям:
- Дата события;
- Тип сообщения;
- Кто делал;
- Что сделали;
- Объект, над которым производится действие;
- Имя роли;
- Откуда подключались;
- Информация об агенте подключения.

При детализации строки выводится дополнительная информация:
- Имя vcenter;
- Сообщение.

По всем колонкам доступна сортировка данных для удобства пользования.

- **Действия с виртуальными машинами** (рис.22):

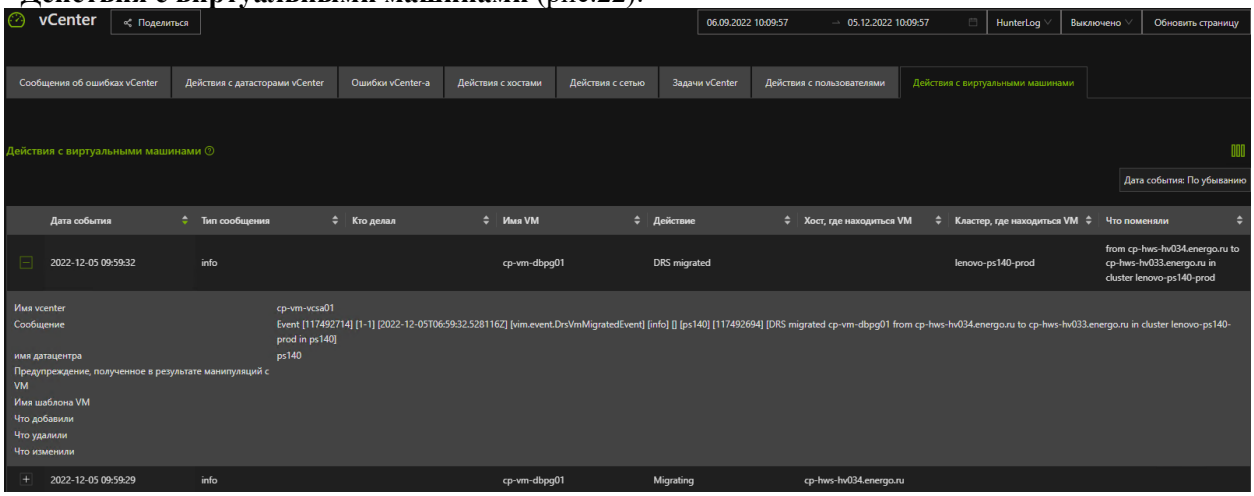

Рис.22

На странице представлены все действия с виртуальными машинами за выбранный период. Пользователю доступна информация по следующим полям:
- Дата события;
- Тип сообщения;
- Кто делал;
- Имя VM;
- Действие;
- Хост, где находится VM;
- Кластер, где находится VM;
- Что поменяли.

При детализации строки пользователю доступна более подробная информация по каждому событию, представленная следующими данными:
- Имя vcenter;
- Сообщение;
- Имя датацентра;
- Предупреждение, полученное в результате манипуляций с VM;
- Имя шаблона VM;
- Что добавили;
- Что удалили;
- Что изменили.

По всем колонкам доступна сортировка данных для удобства пользования.

Exchange:

Раздел «Exchange» состоит из трех подразделов «Мобильные клиенты», «Системные события Exchange» и «Отслеживание писем Exchange». Подробная информация о каждом разделе представлена ниже.

«Мобильные клиенты»

Данный подраздел представлен в виде следующих вкладок:

- **События ActiveSync** (рис.23):

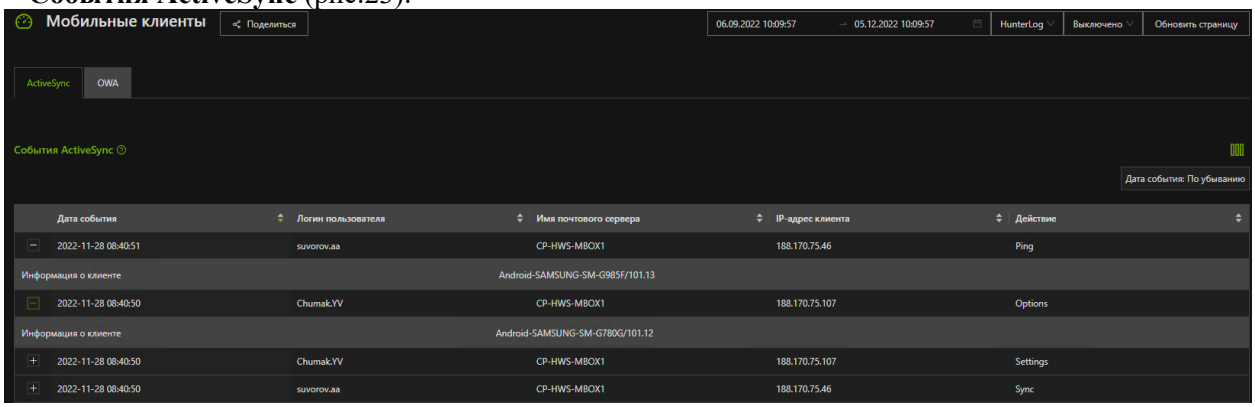

Рис.23

Данные события – это, подключения к Microsoft Exchange OWA от мобильных клиентов по протоколу ActiveSync.

Информация на странице представлена в разрезе следующих полей:
- Дата события;
- Логин пользователя;
- Имя почтового сервера;
- IP-адрес клиента;
- Действие.

При детализации строки, отображается информация о клиенте, которое участвует в событии.

- **Аудит OWA** (рис.24):

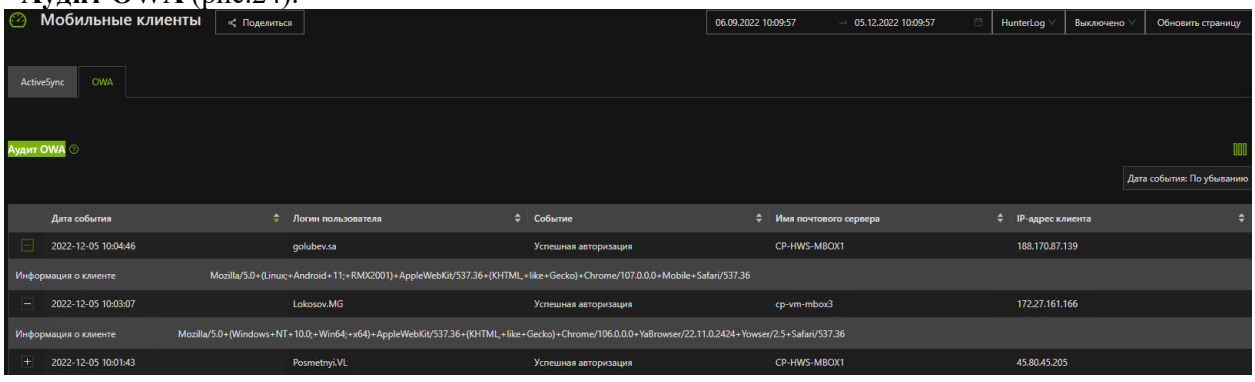

Рис.24

На странице представлены события по подключению к Microsoft Exchange OWA через веб-интерфейс.
Представление информации по следующим полям:
- Дата события;
- Логин пользователя;
- Событие;
- Имя почтового сервера;
- IP-адрес клиента.

При детализации строки, отображается информация о клиенте, которое участвует в событии.

«Системные события Exchange»

Данный подраздел представлен в виде следующих вкладок:

- Репликация DAG Exchange (рис.25):

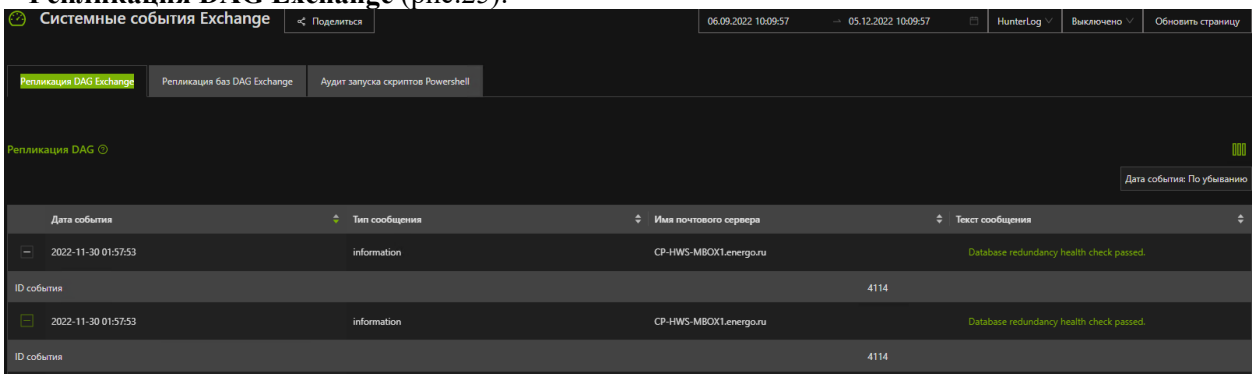

Рис.25

На данной странице представлены логи репликации групп доступности (DAG). Данные представлены в виде:
- Дата события;
- Тип сообщения;
- Имя почтового сервера;
- Текст сообщения.

При детализации строки выводится ID события.

- Репликация баз DAG Exchange (рис.26):

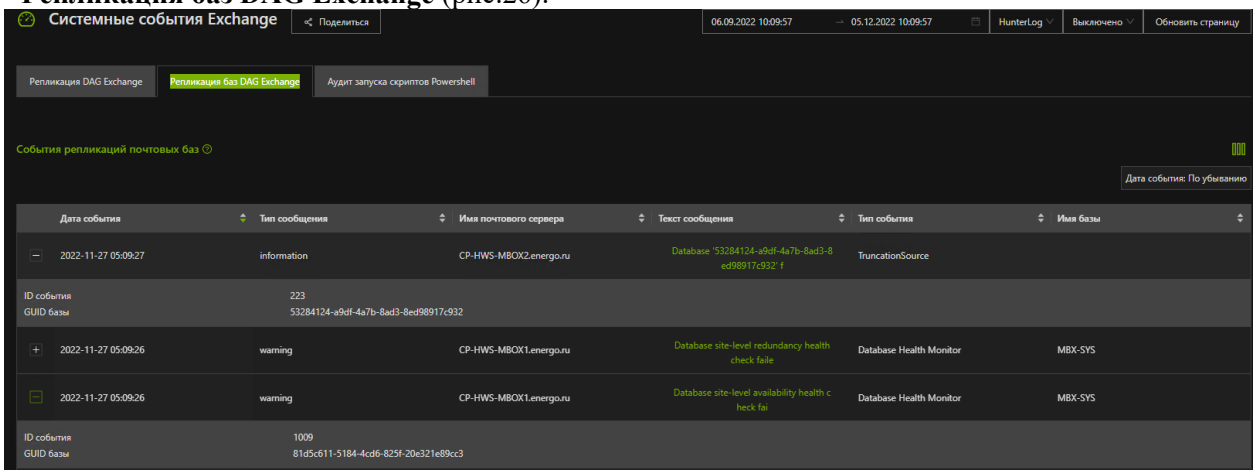

Рис.26

На данной странице представлены логи репликации групп доступности (DAG). Данные представлены в виде:
- Дата события;
- Тип сообщения;
- Имя почтового сервера;
- Текст сообщения;
- Тип события;
- Имя базы.

При детализации строки выводятся ID события и GUID базы.

- Аудит запуска скриптов Powershell (рис.27):

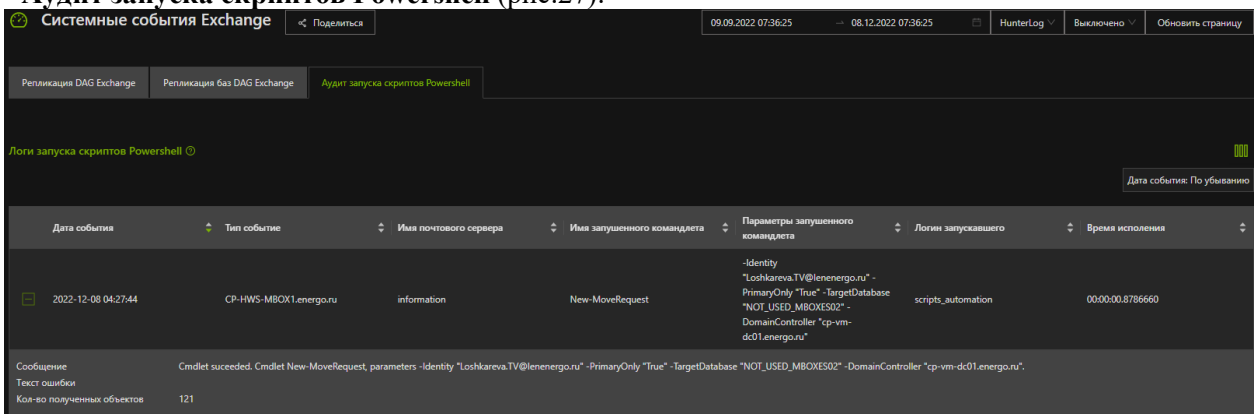

Рис.27

На данной странице представлены все логи запускаемых скриптов Powershell. Данные представлены в виде:
- Дата события;
- Тип события;
- Имя почтового сервера;
- Имя запушенного командлета;
- Параметры запушенного командлета;
- Логин запускавшего;
- Время исполнения.

При детализации строки пользователю доступны дополнительные данные:
- Сообщение;
- Текст ошибки;
- Количество полученных объектов.

«Отслеживание писем Exchange»

Данный подраздел представлен в виде следующих вкладок:

- Отслеживание писем Exchange (рис.28):

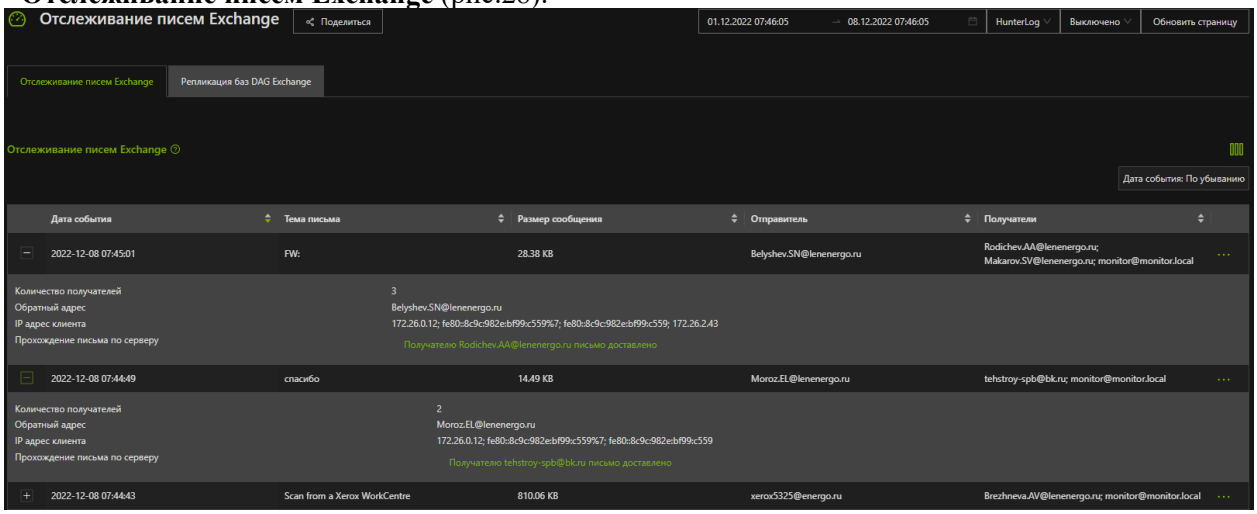

Рис. 28

На данной странице пользователю представлена подробная информация об отправляемых письмах:
- Дата события;
- Тема события;

- Размер сообщения;
- Отправитель;
- Получатель.

В конце каждой строки при наведении курсора мыши на «…» выводится ID сообщения, при нажатии на них автоматически происходит переход на вкладку с логами по выбранному message id (рис.29):

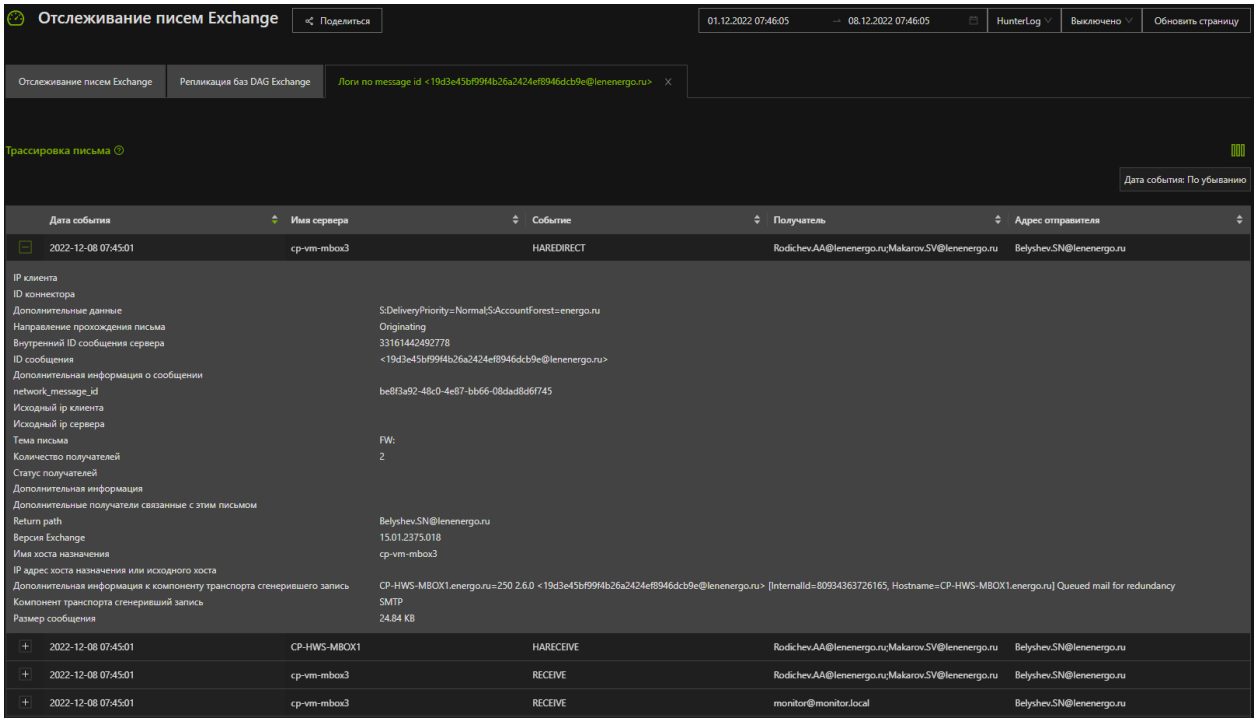

Рис.29

При детализации строки выводится дополнительная информация:
- Количество получателей;
- Обратный адрес;
- IP-адрес клиента;
- Прохождение письма по серверу – при нажатии на данные, открывается окно, в котором перечислены статусы по каждому получателю письма;

- **Репликация баз DAG Exchange** (рис.30):

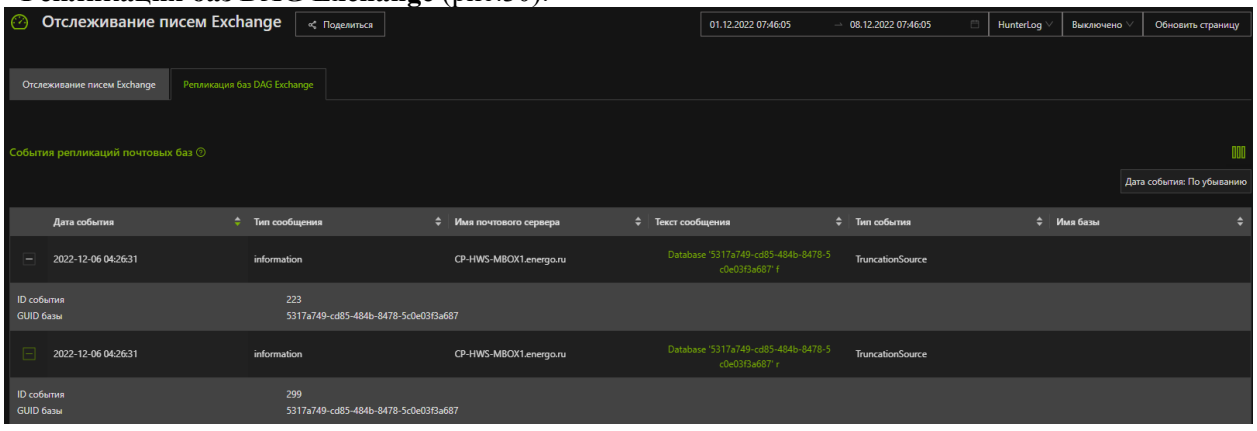

Рис. 30

На данной странице представлены логи событий репликаций почтовых баз (DAG):
- Дата события;
- Тип сообщения;
- Имя почтового сервера;
- Текст сообщения – при нажатии на сообщение, открывается полный запрос;

- Тип события;
- Имя базы.

При детализации строки отображается ID события, а также, GUID базы.

«Linux»

Данный подраздел включает в себя информацию по аудиту подключений к Linux, аудиту изменений файловой системы, истории выполняемых команд и изменению учетных записей:

- **Аудит подключений к Linux** (рис.31):

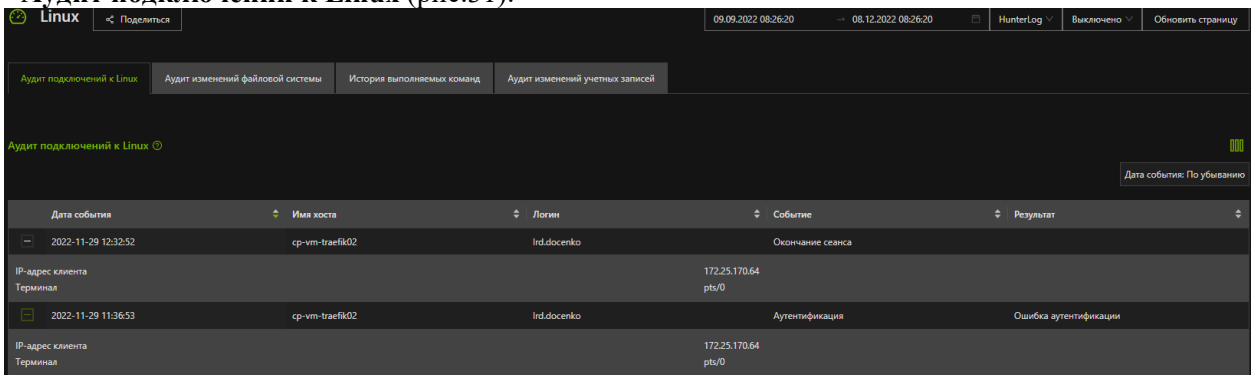

Рис.31

На странице представлены все события подключений за выбранный период:
- Дата события;
- Имя хоста;
- Логин;
- Событие;
- Результат.

При детализации строки выводится информация по IP-адресу клиента и терминале.

- **Аудит изменений файловой системы** (рис.32):

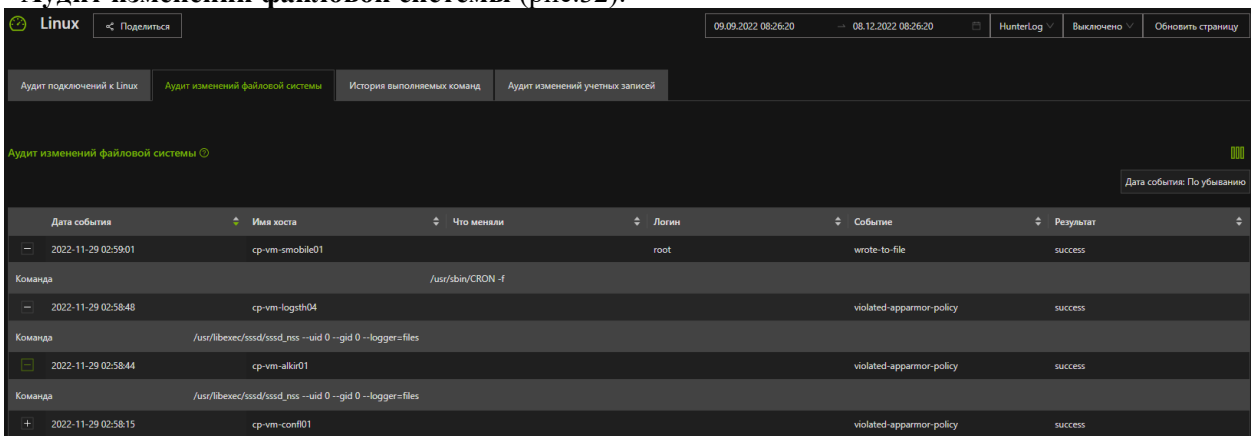

Рис.32

На странице представлены события изменений файловой системы за выбранный период:
- Дата события;
- Имя хоста;
- Что меняли;
- Логин;
- Событие;
- Результат.

При детализации строки выводится выполненная команда.

- **История выполненных команд** (рис.33):

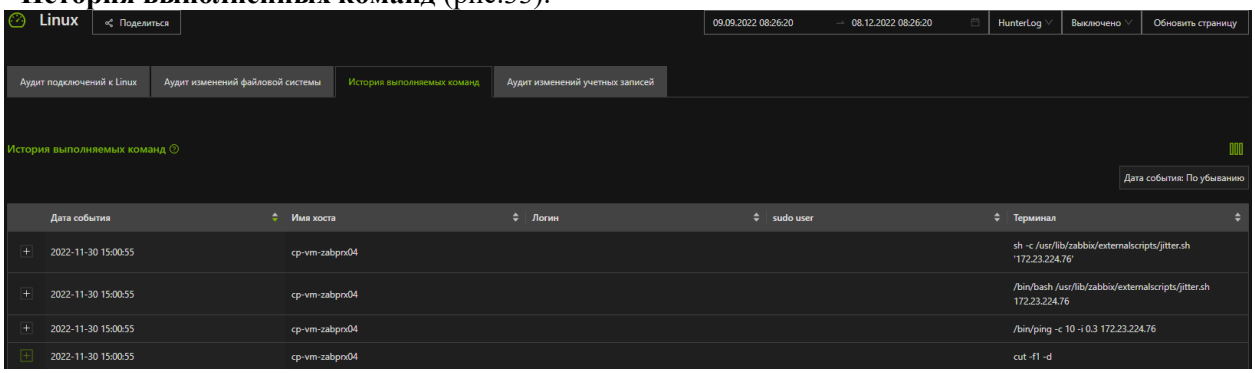

Рис.33

На странице представлена вся история выполненных команд за выбранный период:
- Дата события;
- Имя хоста;
- Логин;
- sudo user;
- Терминал.

- **Аудит изменений учетных записей** (рис.34):

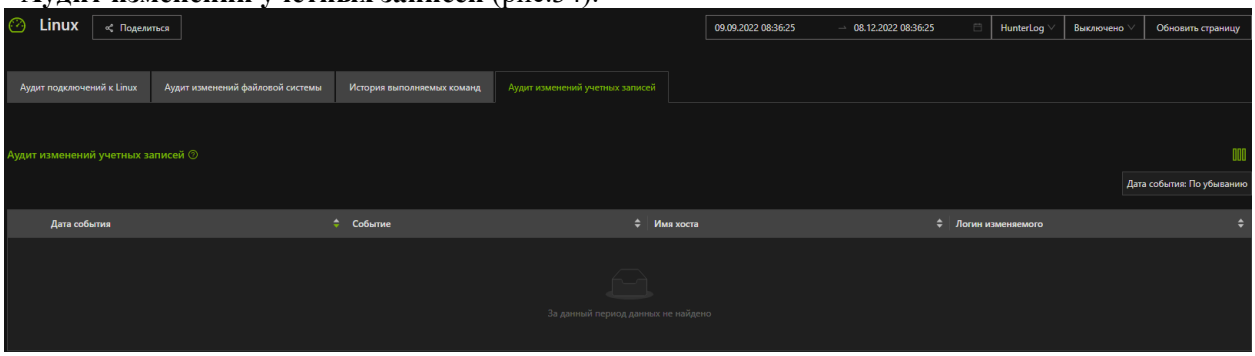

Рис.34

На странице представлена вся информация по изменению учетных записей за выбранный период:
- Дата события;
- Событие;
- Имя хоста;
- Логин изменяемого.

За текущий период изменений учетных записей не происходило.

«Локальный компьютер»

Данный подраздел включает в себя всю информацию по аудиту действий на локальных компьютерах и состоит из следующих подразделов:

- **События приложений** (рис.35):

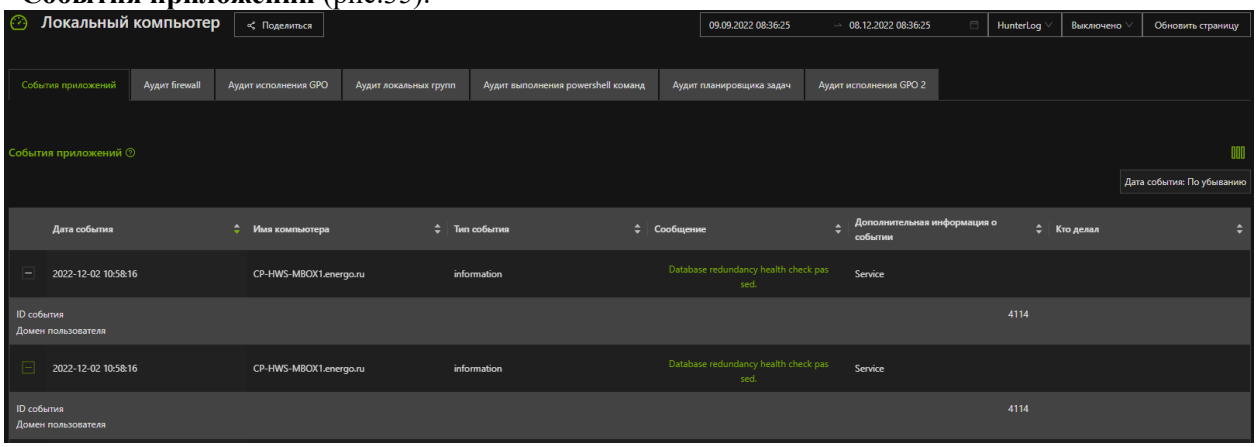

Рис.35

На странице представлены все события журнала приложений Windows за выбранный период:
- Дата события;
- Имя компьютера;
- Тип события;
- Сообщение – при нажатии на текст, открывается окно с текстом запроса и возможностью его копирования;
- Дополнительная информация о событии;
- Кто делал.

При детализации строки выводится информация по ID события и домену пользователя.

- **Аудит Firewall** (рис.36):

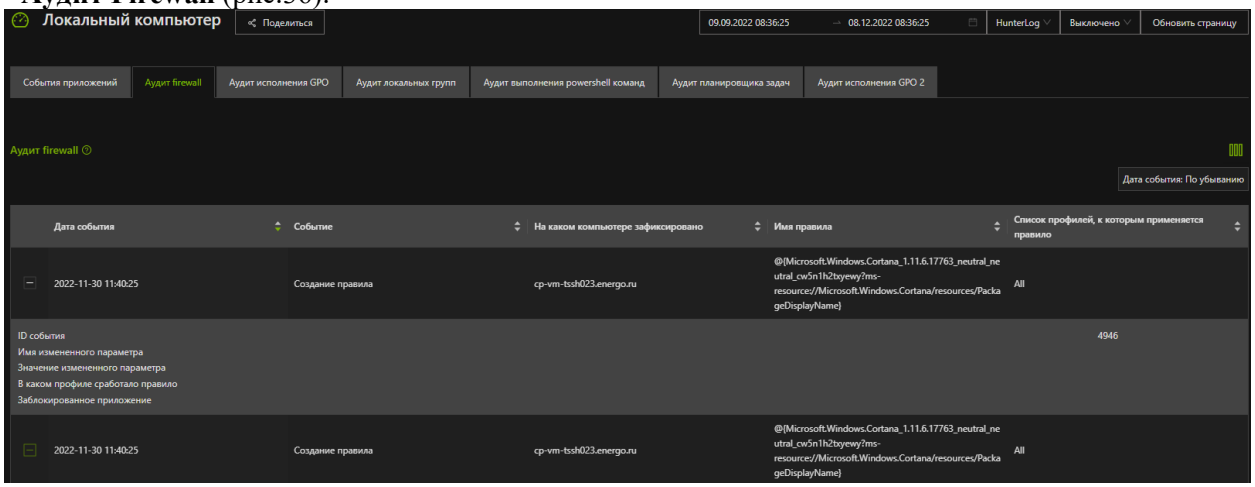

Рис.36

На странице представлены все события брандмауэра Windows за выбранный период:
- Дата события;
- Событие;
- На каком компьютере зафиксировано;
- Имя правила;
- Список профилей, к которым применяется правило.

При детализации строки выводится дополнительная информация по событию:
- ID события;
- Имя измененного параметра;
- Значение измененного параметра;
- В каком профиле сработало правило;
- Заблокированное приложение.

- **Аудит исполнения GPO** (рис.37):

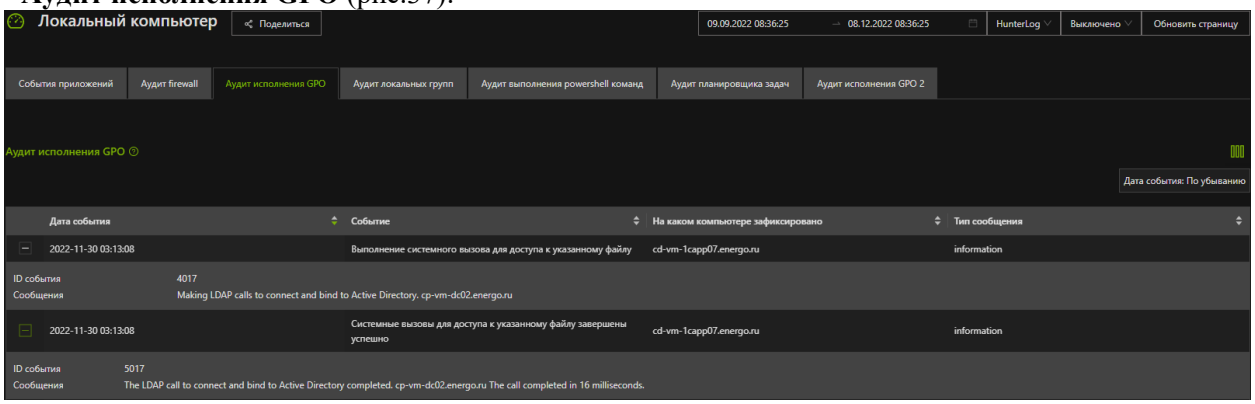

Рис.37

На странице представлены аудит всех событий изменения групповых политик за выбранный период:
- Дата события;
- Событие;
- На каком компьютере зафиксировано;
- Тип сообщения.

При детализации строки выводится дополнительная информация по ID события и сообщению.

- **Аудит локальных групп** (рис.38):

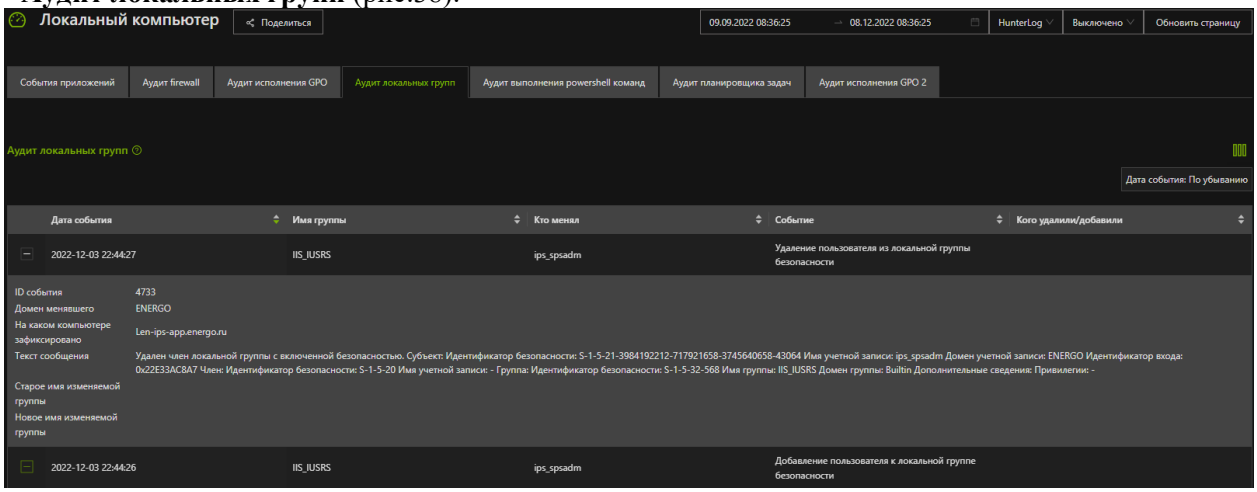

Рис.38

На странице представлены аудит всех изменений локальных групп на компьютере за выбранный период:
- Дата события;
- Имя группы;
- Кто менял;
- Событие;
- Кого удалили/добавили.

При детализации строки выводится дополнительная информация:
- ID события;
- Домен менявшего;
- На каком компьютере зафиксировано;
- Текст сообщения;
- Старое имя изменяемой группы;
- Новое имя изменяемой группы.

- **Аудит выполнения Powershell команд** (рис.39):

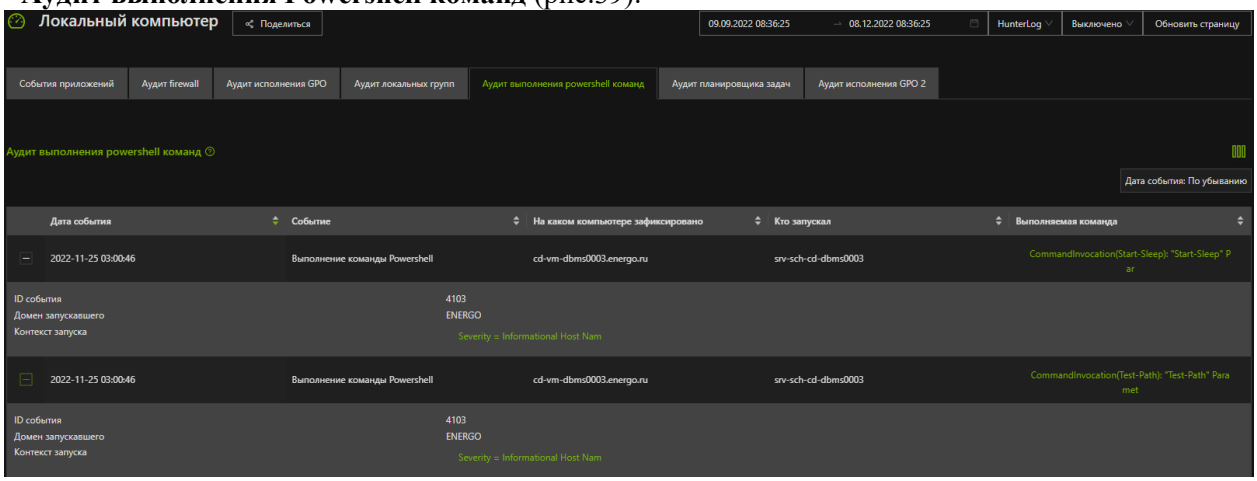

Рис.39

На странице представлены аудит всех выполняемых команд в командной строке на компьютере за выбранный период:
- Дата события;
- Событие;
- На каком компьютере зафиксировано;
- Кто запускал;
- Выполняемая команда – при нажатии на текст команды, откроется окно с полным текстом команды и возможностью его копирования.

При детализации строки выводится дополнительная информация:
- ID события;
- Домен запускавшего;
- Контекст запуска – при нажатии на контекст команды, откроется окно с полным текстом и возможностью его копирования.

- **Аудит планировщика задач** (рис.40):

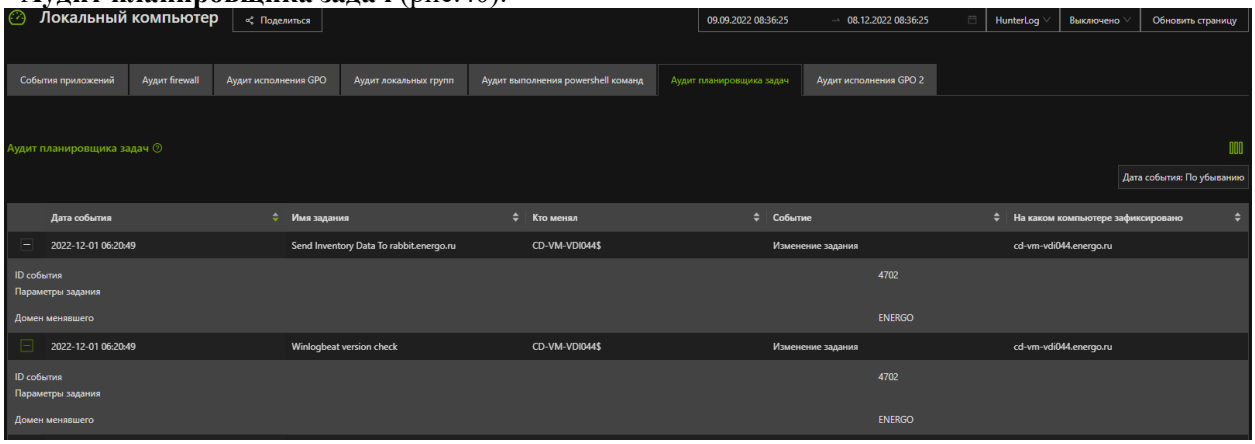

Рис.40

На странице представлены аудит всех зафиксированных событий в планировщике задач на компьютере за выбранный период:
- Дата события;
- Имя задания;
- Кто менял;
- Событие;
- На каком компьютере зафиксировано.

При детализации строки выводится дополнительная информация:
- ID события;
- Параметры задания;
- Домен менявшего.

- **Аудит исполнения GPO 2** (рис.41):

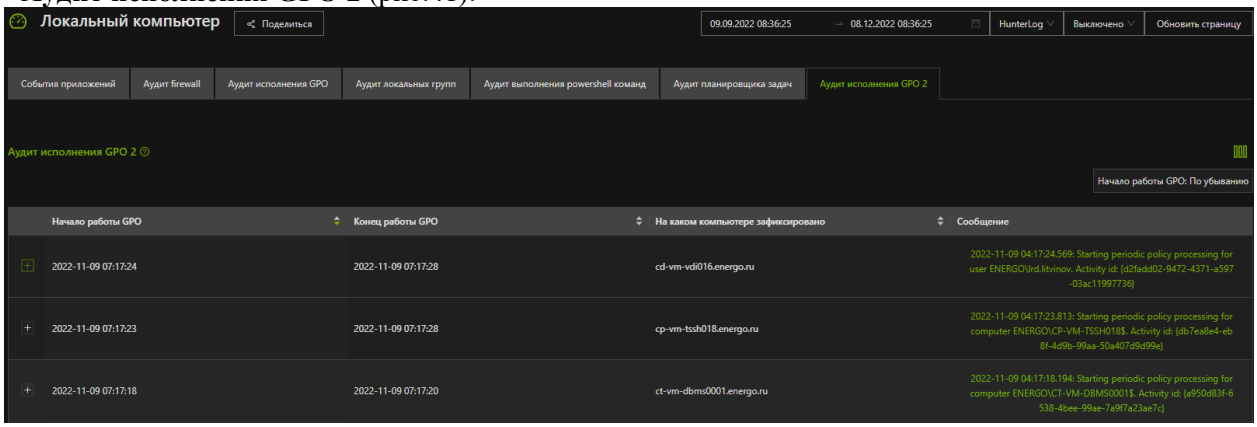

Рис.41

На странице представлен расширенный аудит всех событий изменения групповых политик за выбранный период:
- Начало работы GPO;
- Конец работы GPO;
- На каком компьютере зафиксировано;
- Сообщение – при нажатии на часть текста сообщения, откроется окно с полным текстом данного сообщения и возможностью его копирования (рис.42).

Рис.42

«NetFlow»

Данный подраздел включает в себя всю информацию по учету сетевого трафика (рис.43).

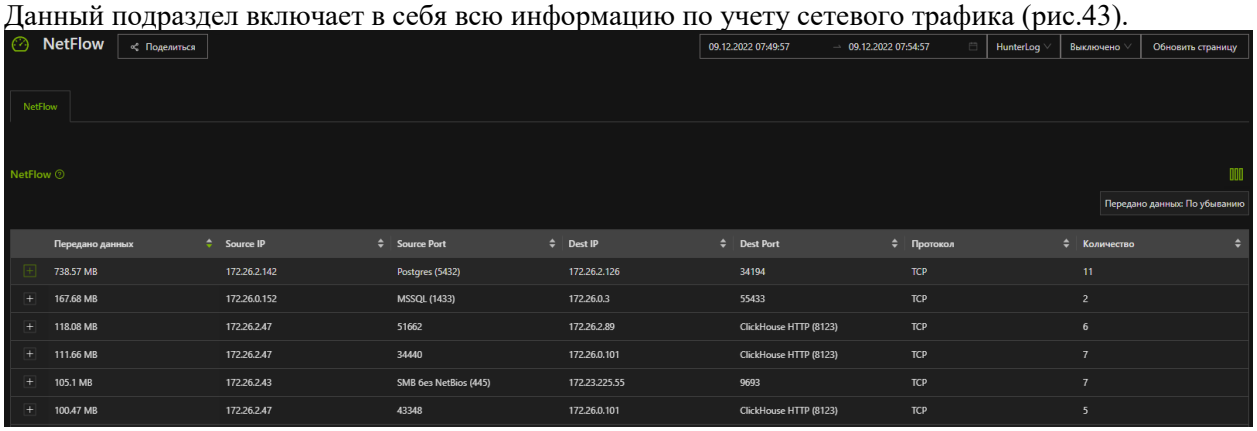

Рис.43

На странице сгруппированы данные по следующим полям:
- Передано данных (MB);
- Source IP;
- Source Port;
- Dest IP;
- Dest Port;
- Протокол;
- Количество.

Для удобства использования, по каждой колонке доступна сортировка данных.

«VPN»

Данный подраздел включает в себя всю информацию по учету трафика подключений по VPN (рис.44).

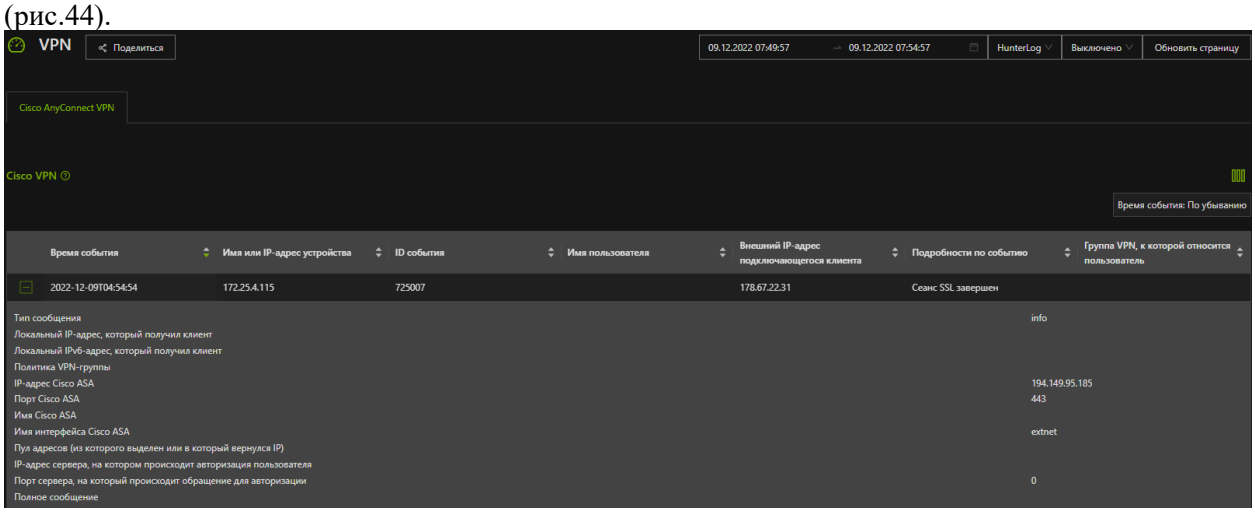

Рис.44

На странице сгруппированы данные по следующим полям:
- 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.

При детализации строки реализован дополнительны свод информации, состоящий из:
- Тип сообщения;
- Локальный IP-адрес, который получил клиент;
- Локальный IPv6-адрес, который получил клиент;
- Политика VPN-группы;
- IP-адрес Cisco ASA;
- Порт Cisco ASA;
- Имя Cisco ASA;
- Имя интерфейса Cisco ASA;
- Пул адресов (из которого выделен или в который вернулся IP);
- IP-адрес сервера, на котором происходит авторизация пользователя;
- Порт сервера, на который происходит обращение для авторизации;
- Полное сообщение.

«Сетевые папки»

Данный подраздел включает в себя всю информацию по учету действий с сетевыми папками (рис.45).

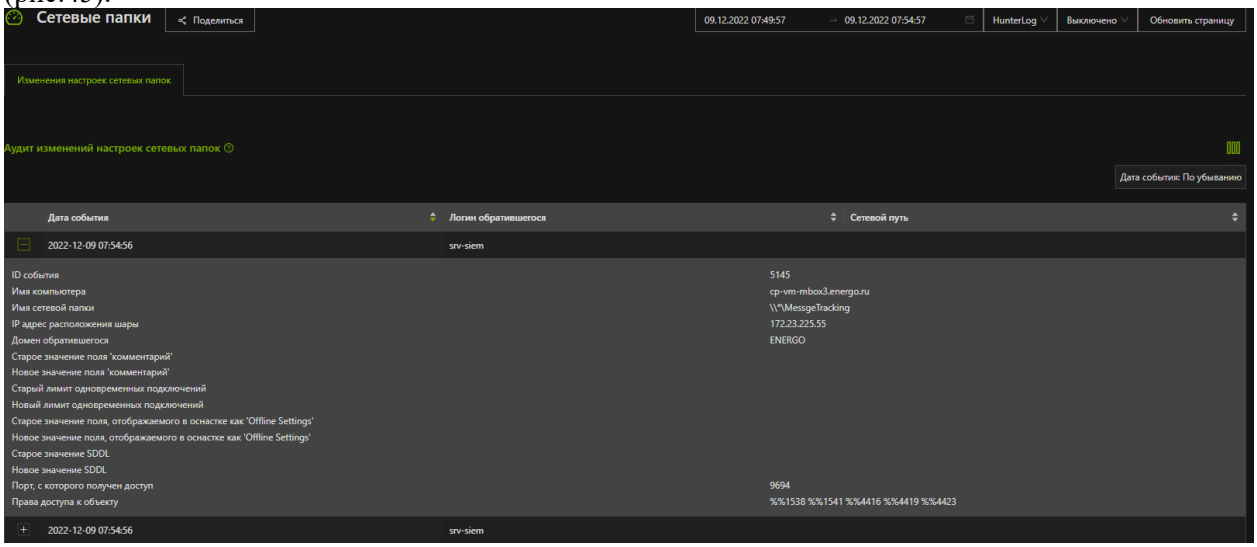

Рис.45

События выводятся за выбранный пользователем период с группировкой по дате события, логину обратившегося и сетевому пути. При детализации каждой строки реализовано получение подробных данных по выбранному событию:

- ID события;
- Имя компьютера;
- Имя сетевой папки;
- IP адрес расположения шары;
- Домен обратившегося;
- Старое значение поля 'комментарий';
- Новое значение поля 'комментарий';
- Старый лимит одновременных подключений;
- Старое значение поля, отображаемого в оснастке как 'Offline Settings';
- Новое значение поля, отображаемого в оснастке как 'Offline Settings';
- Старое значение SDDL;
- Новое значение SDDL;
- Порт, с которого получен доступ;
- Права доступа к объекту.

Для удобства использования информации реализована сортировка, как по колонкам, так и по дате.

4. 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.