|  |  |  |
| --- | --- | --- |
| УТВЕРЖДАЮ  Директор ООО "Активные Технологии"  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П.А. Гончар  "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |  | УТВЕРЖДАЮ  ЗАО «Специальная финансовая организация «Центр секьюритизации»    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.Г. Дубина  "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |

**ТЕХНИЧЕСКИЙ ОТЧЕТ**

**ИСПЫТАНИЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ**

**ИНФОРМАЦИОННОЙ СИСТЕМЫ  
«Учет операций секьюритизации»**

2022СОДЕРЖАНИЕ

[1. ВВЕДЕНИЕ](#_Toc86678358)

[2. ОПИСАНИЕ ОБЪЕКТА ОЦЕНКИ 3](#_Toc86678359)

[2.1. Общие сведения 3](#_Toc86678360)

[2.2. Описание границ объекта оценки 4](#_Toc86678361)

[2.2.1. Физическая граница объекта оценки 4](#_Toc86678362)

[2.2.2. Логическая граница объекта оценки 4](#_Toc86678363)

[3. РЕЗУЛЬТАТЫ ИСПЫТАНИЙ 5](#_Toc86678364)

[4. ВЫВОДЫ И РЕКОМЕНДАЦИИ 5](#_Toc86678365)

[5. СПИСОК ПРЕДСТАВЛЕННЫХ МАТЕРИАЛОВ 5](#_Toc86678366)

[6. ОТЧЕТ НАБЛЮДЕНИЙ. ПРОВЕРКА ВЫПОЛНЕНИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ 7](#_Toc86678367)

[6.1. Проверка реализации требований по обеспечению аудита безопасности 9](#_Toc86678368)

[6.2.Проверка реализации требований по обеспечению защиты данных 16](#_Toc86678369)

[6.3.Проверка реализации требований по обеспечению идентификации и аутентификации 22](#_Toc86678370)

[6.4. Проверка реализации требований по обеспечению защиты системы защиты информации ИС 32](#_Toc86678371)

[6.5.Проверка реализации требований по обеспечению криптографической защиты информации 38](#_Toc86678372)

[6.6.Проверка реализации дополнительных требований по обеспечению защиты информации в виртуальной инфраструктуре 41](#_Toc86678373)

[6.7.Проверка реализации иных требований 44](#_Toc86678374)

[7. ОТЧЕТ О ВНЕШНЕЙ И ВНУТРЕННЕЙ ПРОВЕРКЕ ОТСУТСТВИЯ ЛИБО НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ НАРУШИТЕЛЕМ СВОЙСТВ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ И АППАРАТНЫХ СРЕДСТВ 50](#_Toc86678375)

1. ВВЕДЕНИЕ

**Объект оценки:** Информационная система «Центр секьюритизации»

**Сведения о методике аттестации:** Методика аттестации системы защиты информации информационной системы «Учет операций секьюритизации», утвержденная 24.12.2022г.

**Наименование и реквизиты собственника информационной системы:**

ЗАО «Специальная финансовая организация «Центр секьюритизации», 220114, г. Минск, ул. Филимонова, 25Г-211 р/с BY21BAPB30117144300100000000 в ОАО «Белагропромбанк», БИК BAPBBY2X УНП 193351501

**Цель испытаний:** документальное подтверждение соответствия системы защиты информации информационной системы «Учет операций секьюритизации» (далее – ИС) требованиям законодательства Республики Беларусь об информации, информатизации и защите информации, а также, содержащимся в документе «Система защиты информации информационной системы «Учет операций секьюритизации». Техническое задание» (далее – ТЗ), и выдача на этой основе аттестата соответствия системы защиты информации ИС требованиям по защите информации.

**Обозначение НПА, устанавливающего требования к объекту оценки:**

* Закон Республики Беларусь от 10 ноября 2008 года № 455-З (ред. от 11.05.2016) «Об информации, информатизации и защите информации»;
* Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденное приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66.

**Место проведения испытаний:** на площадях ЗАО «Специальная финансовая организация «Центр секьюритизации»

**Сроки проведения испытаний:** 21.02.2022 – 28.02.2022

**2. ОПИСАНИЕ ОБЪЕКТА ОЦЕНКИ**

**2.1. Общие сведения**

В состав ИС входит сервера MySQL Server, itVPN Server, Web Server, ESET Remote administrator Server, Syslog Server, маршрутизатор gw\_centrsecuritization-01, маршрутизатор SEC-GATE, маршрутизатор SEC-RT, автоматизированное рабочее место пользователя.

Автоматизированное рабочее место пользователя располагается в офисе по адресу: г. Минск, ул. Филимонова 25-Г, офис.211.

Общая структурная схема ИС представлена на рисунке 1.

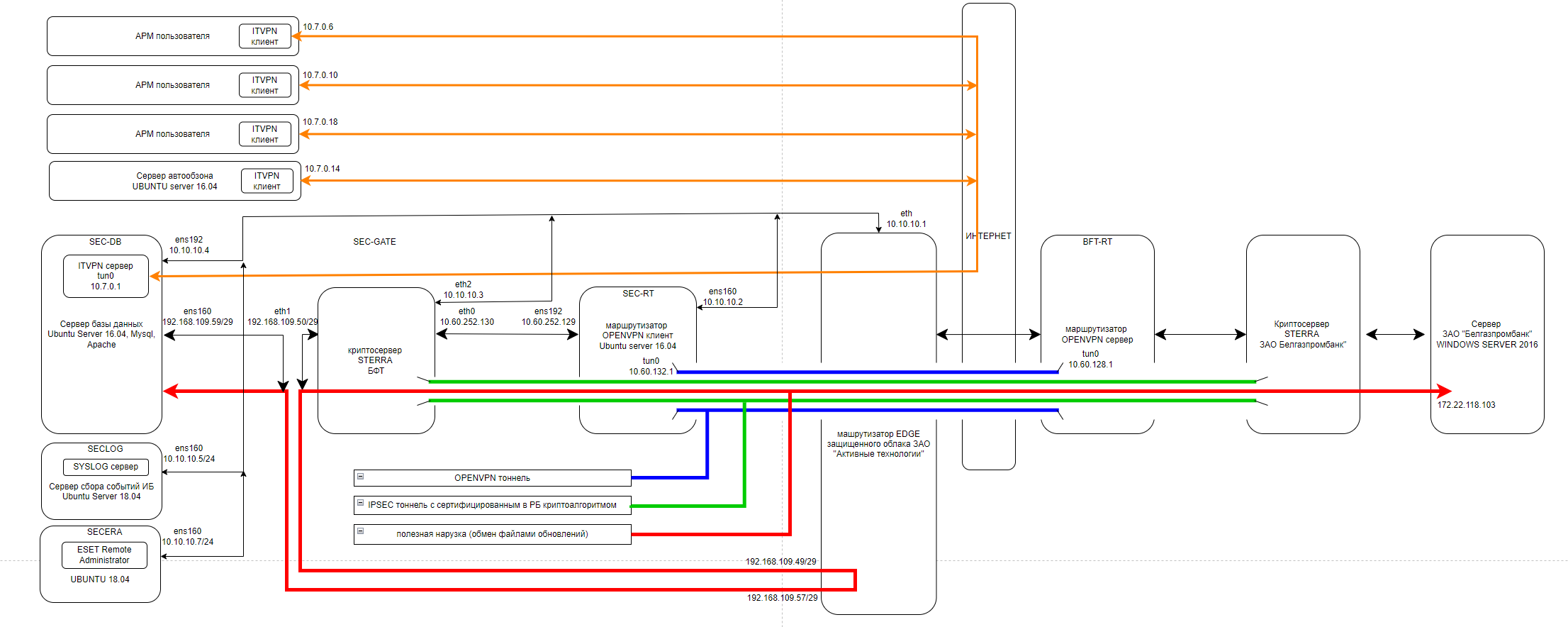


Рисунок 1 – Общая структурная схема ИС

Субъектами ИС являются:

Пользователи ИС «Учет операций секьюритизации»

Защищаемыми активами ИС являются:

Компоненты ИС «Учет операций секьюритизации»

**2.2. Описание границ объекта оценки**

**2.2.1. Физическая граница объекта оценки**

В физические границы ИС входят:

* itVPN Server;
* MySQL Server;
* Syslog Server;
* ESET Remote administrator Server;
* маршрутизатор gw\_centrsecuritization-01;
* маршрутизатор SEC-GATE;
* маршрутизатор SEC-RT.

**2.2.2. Логическая граница объекта оценки**

Логические границы определяются функционалом ИС:

* учет проводимых операций секьюритизации;
* учет эмитированных облигаций в рамках проводимых операций секьюритизации;
* контроль поступления средств в рамках проводимых операций секьюритизации;
* контроль расчетов по эмитированным облигациям в рамках проводимых операций секьюритизации;
* учет расходов в рамках проводимых операций секьюритизации;
* контроль просроченной задолженности по операциям секьюритизации на этапах досудебной и судебной стадии взыскания задолженности в рамках проводимых операций секьюритизации;
* проведение смс информирования, автоматического обзвона и форм документов в рамках проводимой работы по операциям секьюритизации;
* формирование отчетности по операциям секьюритизации.

**3. РЕЗУЛЬТАТЫ ИСПЫТАНИЙ**

Объем испытаний и результаты реализации функций безопасности в средствах защиты информации ИС и прикладном программном обеспечении в реальных условиях эксплуатации приведены в таблицах 3.1.

Таблица 3.1 – Результаты испытаний функций безопасности

|  |  |
| --- | --- |
| **Функции безопасности, реализующие требования** | **Результаты проверки** |
| По обеспечению аудита безопасности | Проверка выполнена успешно |
| По обеспечению защиты данных | Проверка выполнена успешно |
| По обеспечению идентификации и аутентификации | Проверка выполнена успешно |
| По обеспечению защиты системы защиты информации ИС | Проверка выполнена успешно |
| По обеспечению криптографической защиты информации | Проверка выполнена успешно |
| По обеспечению дополнительных требований по обеспечению защиты информации в виртуальной инфраструктуре | Проверка выполнена успешно |
| Иные требования | Проверка выполнена успешно |

**4. ВЫВОДЫ И РЕКОМЕНДАЦИИ**

По результатам испытаний системы защиты информации ИС сделаны следующие выводы:

реальный состав и структура объектов ИС соответствует общей схеме системы защиты информации;

требования по защите информации ИС, установленные законодательством Республики Беларусь, выполнены.

**5. СПИСОК ПРЕДСТАВЛЕННЫХ МАТЕРИАЛОВ**

Состав комплекса технических средств ИС, на которых обрабатывается защищаемая информация и программного обеспечения представлен в таблице 5.1.

Перечень средств защиты, применяемых в системе защиты информации ИС представлен в таблице 5.2.

Таблица 5.1 – Комплекс технических средств ИС

| **Наименование элемента** | **Конфигурация** |
| --- | --- |
| Сервер MySQL Server, itVPN Server, Web Server | 6 CPU, 4 RAM, 260Gb HDD |
| Сервер Syslog Server | 1 CPU, 2 RAM, 66Gb HDD |
| Сервер ESET Remote administrator Server | 1 CPU, 1 RAM, 33Gb HDD |
| Маршрутизатор | gw\_centrsecuritization-01 |
| Маршрутизатор | SEC-GATE |
| Маршрутизатор | SEC-RT |

Таблица 5.2 – Средства защиты информации ИС

| **Наименование** | **Сведения о сертификации в Национальной системе подтверждения соответствия Республики Беларусь** |
| --- | --- |
| Межсетевой экран Palo Alto VM | BY/112 02.02.036 00526 |
| Программно-аппаратный комплекс предотвращения DDoS-атак AntiDDoS8080 | BY/112 02.02.036 00687 |
| Программное средство канального шифрования «itVPN» | BY/112 02.01.036 00621 |
| Программное изделие «ESET endpoint protection» | BY/112 02.01.036 00553 |
| Программное обеспечение резервного копирования и восстановления данных Veeam Backup and Replication | BY/112 02.02.036 00531 |
| Платформа виртуализации VMware vSphere в составе гипервизора VMware ESXi и сервера управления VMware vCenter Server 6.5 | BY/112 02.02.036 00355 |
| Платформа виртуализации и обеспечения безопасности сети VMware NSX версии 6.4 | BY/112 02.02.036 00473 |
| Коммутаторы CE6851-48S6Q-HI серии CloudEngine 6800 2 шт. | BY/112 02.02.036 00764 |

**6. ОТЧЕТ НАБЛЮДЕНИЙ. ПРОВЕРКА ВЫПОЛНЕНИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ**

Для поверки реализации функций безопасности экспертом выполняются требования Методики аттестации системы защиты информации ИС, утвержденной 24.12.2021.

Защита от сетевых атак реализована с использованием программно-аппаратного комплекса предотвращения DDoS-атак AntiDDoS8080 серии AntiDDoS8000 с программным обеспечением V500R001, предоставляемого СООО «Белорусские облачные технологии» согласно приложению №2 к Договору №05-ОДк от 1 августа 2015г. Сертификат представлен на рисунке 6.1



Рисунок 6.1 – Сертификат соответствия на комплекс предотвращения DDoS-атак AntiDDoS8080.

Межсетевое экранирование, предотвращение атак и вторжений реализовано с использованием межсетевого экрана Palo Alto VM под управлением программного обеспечения PAN-OS версии 8.0 в среде виртуализации VMware, предоставляемого СООО «Белорусские облачные технологии» согласно приложению №2 к Договору №05-ОДк от 1 августа 2015г. Сертификат представлен на рисунке 6.2

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 6.2 – Сертификат соответствия на межсетевой экран Palo Alto VM под управлением программного обеспечения PAN-OS версии 8.0

**6.1. Проверка реализации требований по обеспечению аудита безопасности**

Средства программного обеспечения, операционной системы, а также средства технической защиты информации должны позволять:

определять состав информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности и другое);

обеспечивать сбор и хранение информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года;

проводить мониторинг (просмотр, анализ) событий информационной безопасности уполномоченными на это пользователями ИС;

обеспечивать сбор и хранение информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года.

**ПРОЦЕДУРА ТЕСТИРОВАНИЯ:**

Эксперт удостоверяет, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению аудита безопасности, соответствуют требованиям, заявленным в ТЗ.

Результаты тестирования подтверждены и представлены на рисунках 6.1.1 – 6.1.6.

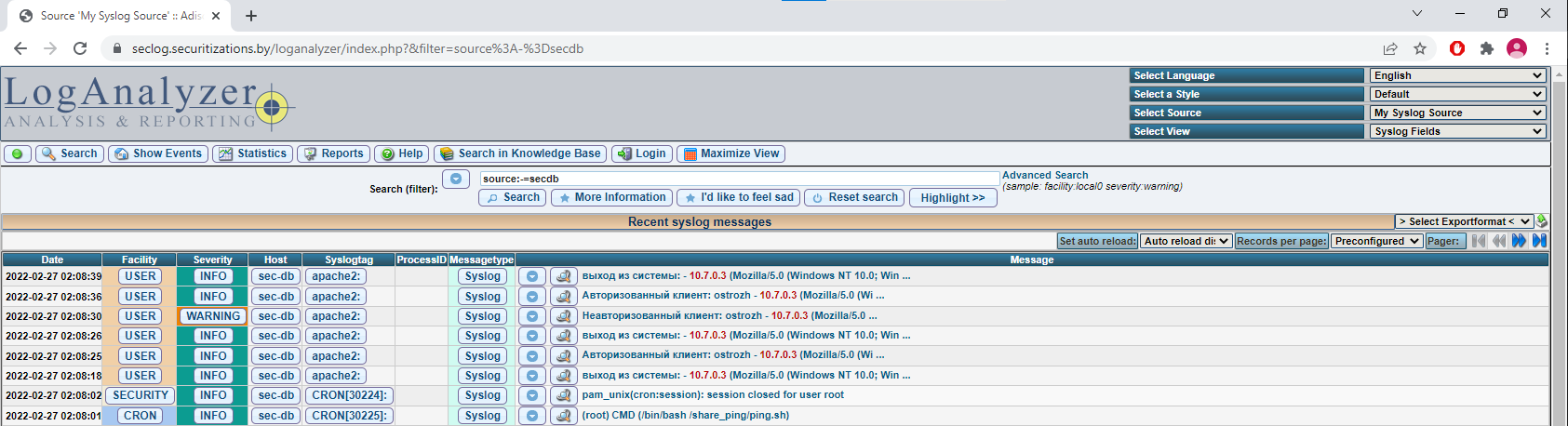


Рисунок 6.1.1 – Информационная система генерирует события аудита. Отображение событий аудита в системе централизованного сбора событий.

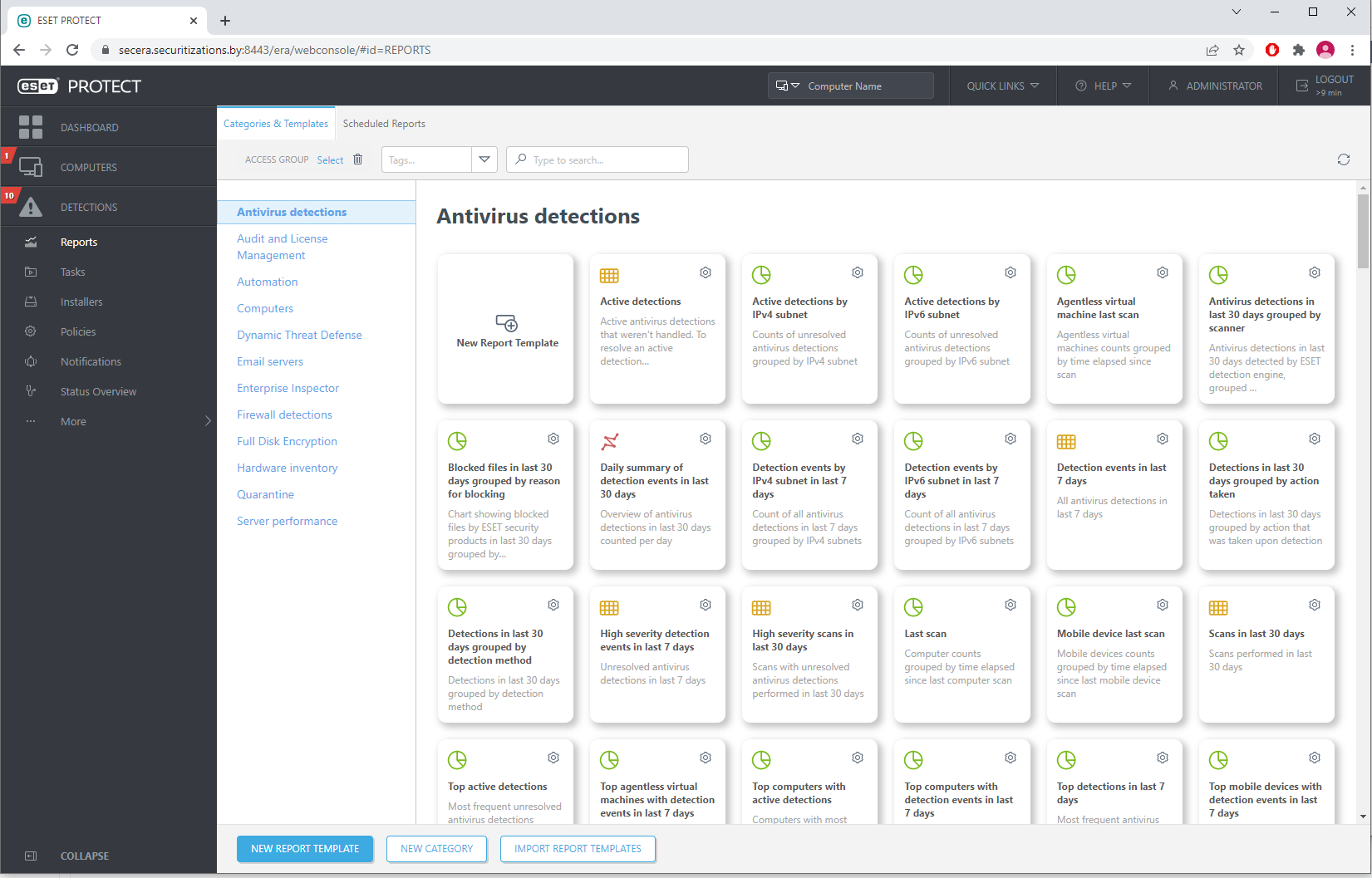


Рисунок 6.1.2 – Настройки отчетов средства защиты информации (антивирусное ПО).

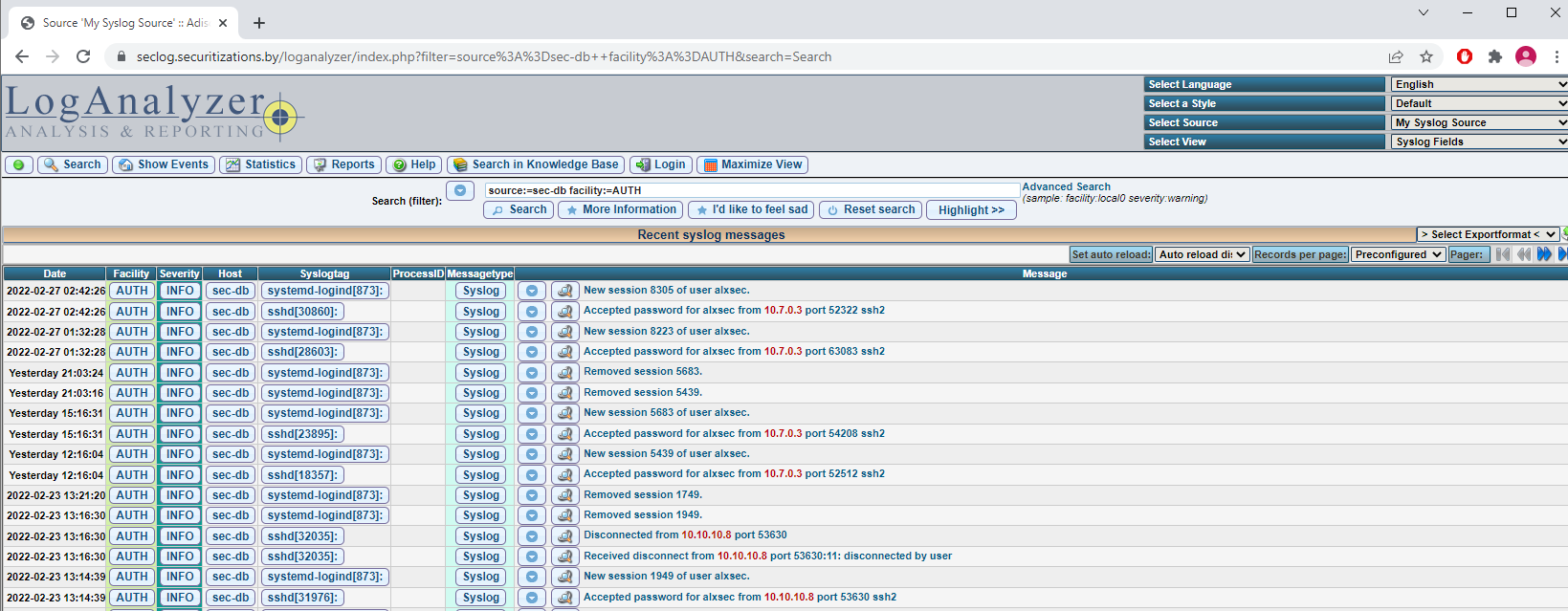


Рисунок 6.1.3 – Настройки отчетов журнала безопасности операционной системы Linux.

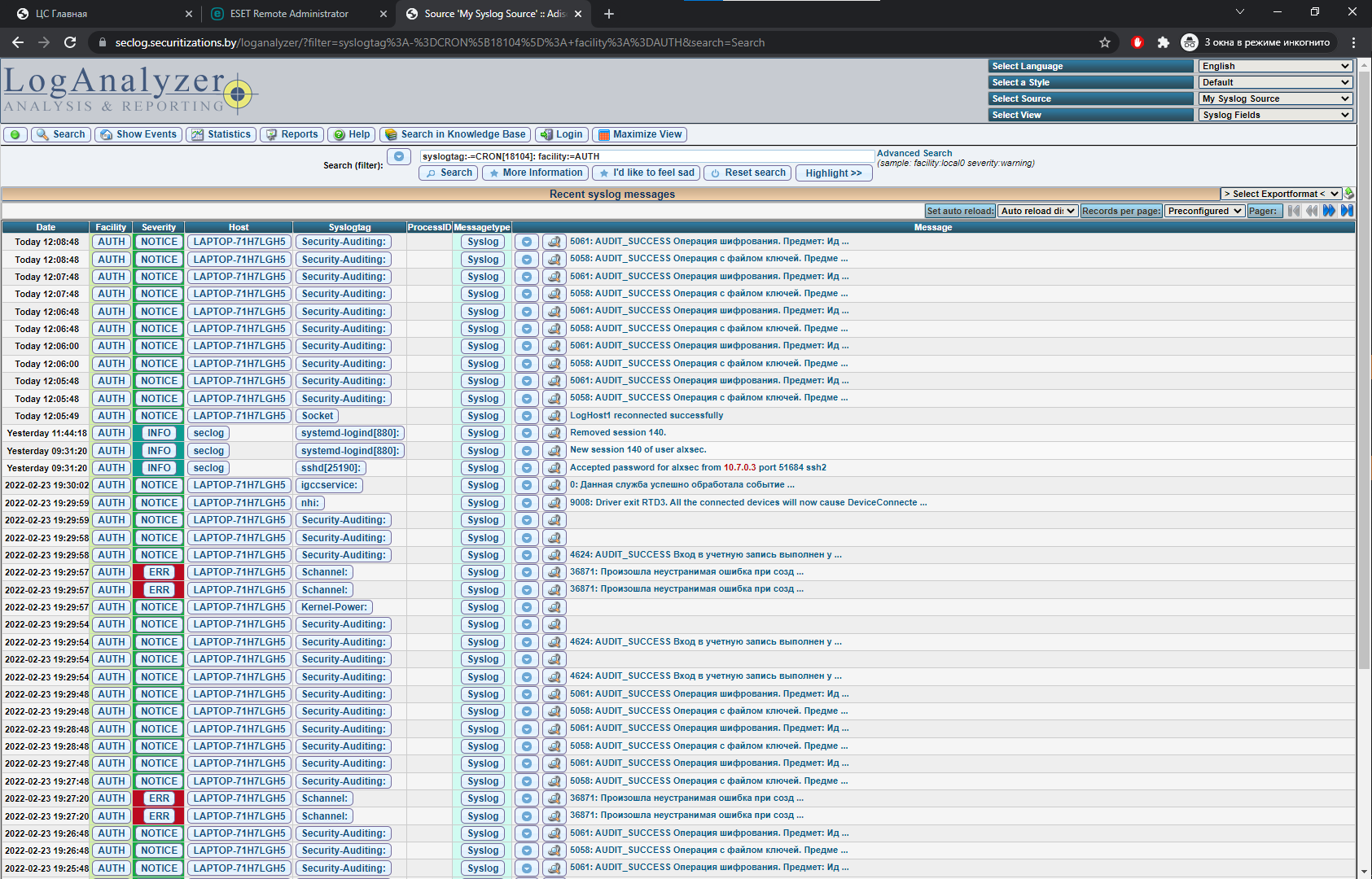


Рисунок 6.1.4 – Syslog сервер собирает события о действиях пользователей.



Рисунок 6.1.5 – Syslog сервер собирает события об обновлениях программного обеспечения.

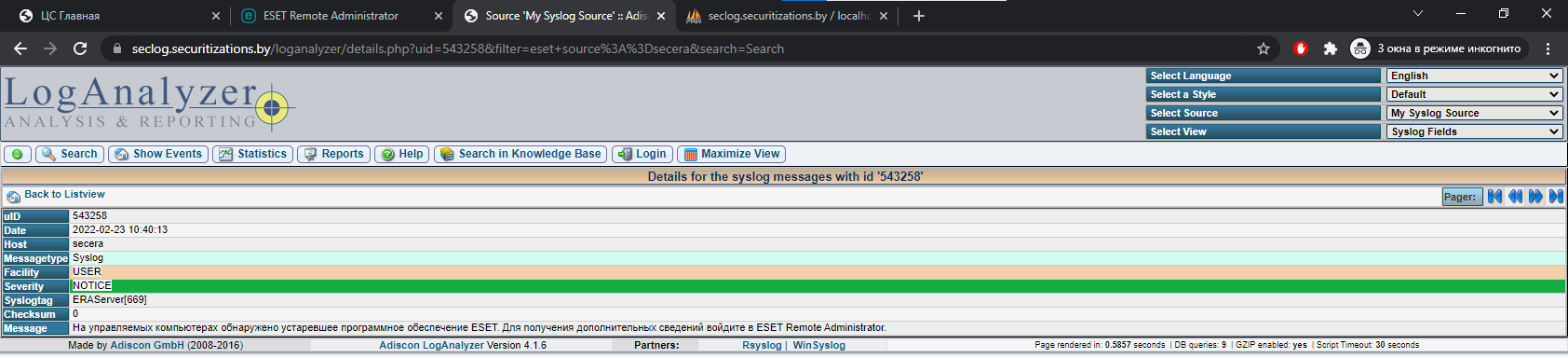


Рисунок 6.1.6 – Syslog сервер собирает события об уведомлениях средств защиты информации.

**УДОСТОВЕРЕНО:**

**Средства программного обеспечения, операционной системы, а также средства технической защиты информации позволяют:**

**определять состав информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности и другое);**

**обеспечивать сбор и хранение информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года;**

**проводить мониторинг (просмотр, анализ) событий информационной безопасности уполномоченными на это пользователями ИС;**

**обеспечивать сбор и хранение информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года.**

**ЗАКЛЮЧЕНИЕ:**

Экспертом удостоверено, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению аудита безопасности, **соответствуют требованиям**, заявленным в ТЗ.

**6.2. Проверка реализации требований по обеспечению защиты данных**

Средства программного обеспечения, операционной системы, а также средства технической защиты информации должны позволять:

контролировать порядок использования в ИС съемных носителей информации, мобильных технических средств;

контролировать работоспособность, параметры настройки и правильность функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации;

обеспечивать защиту от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности.

**ПРОЦЕДУРА ТЕСТИРОВАНИЯ:**

Эксперт удостоверяет, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению защиты данных, соответствуют требованиям, заявленным в ТЗ.

Результаты подтверждены и представлены на рисунках 6.2.1 – 6.2.6.

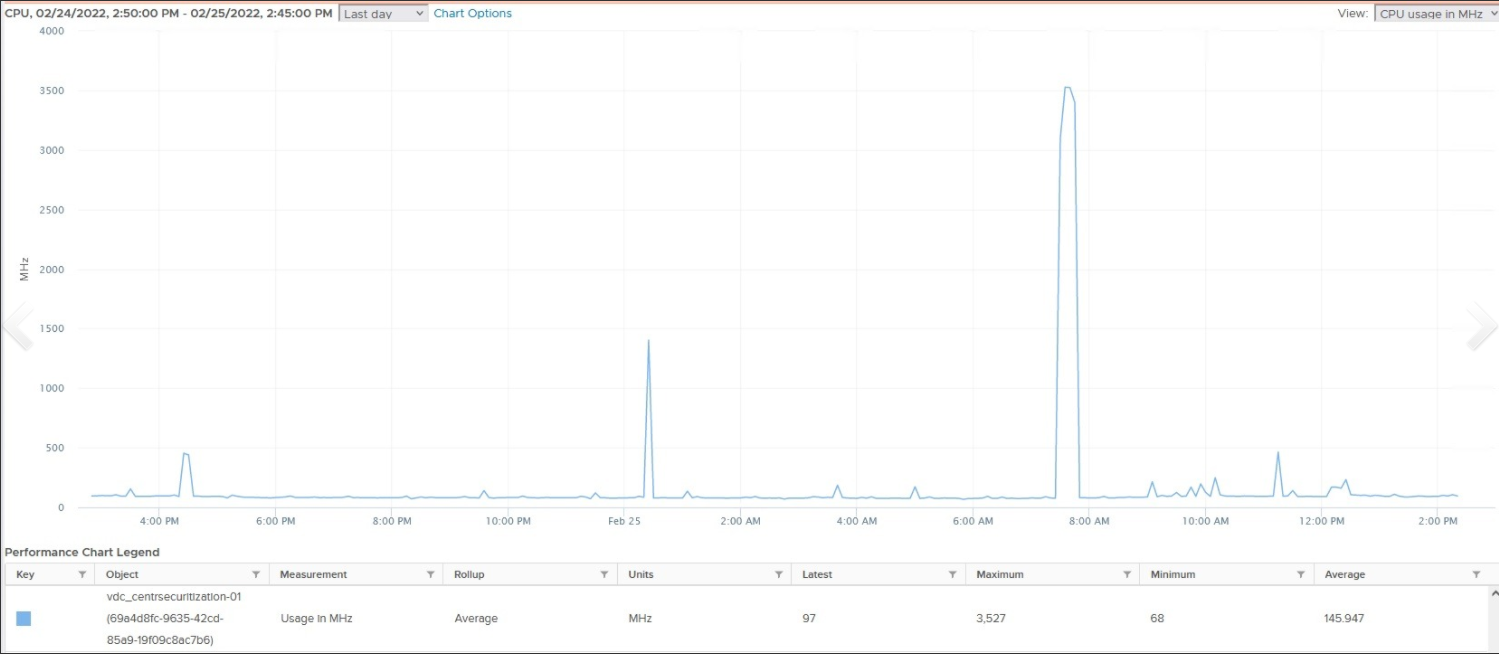


Рисунок 6.2.1 – Контроль за параметрами и правильностью функционирования средств вычислительной техники. График нагрузки на центральный процессор.

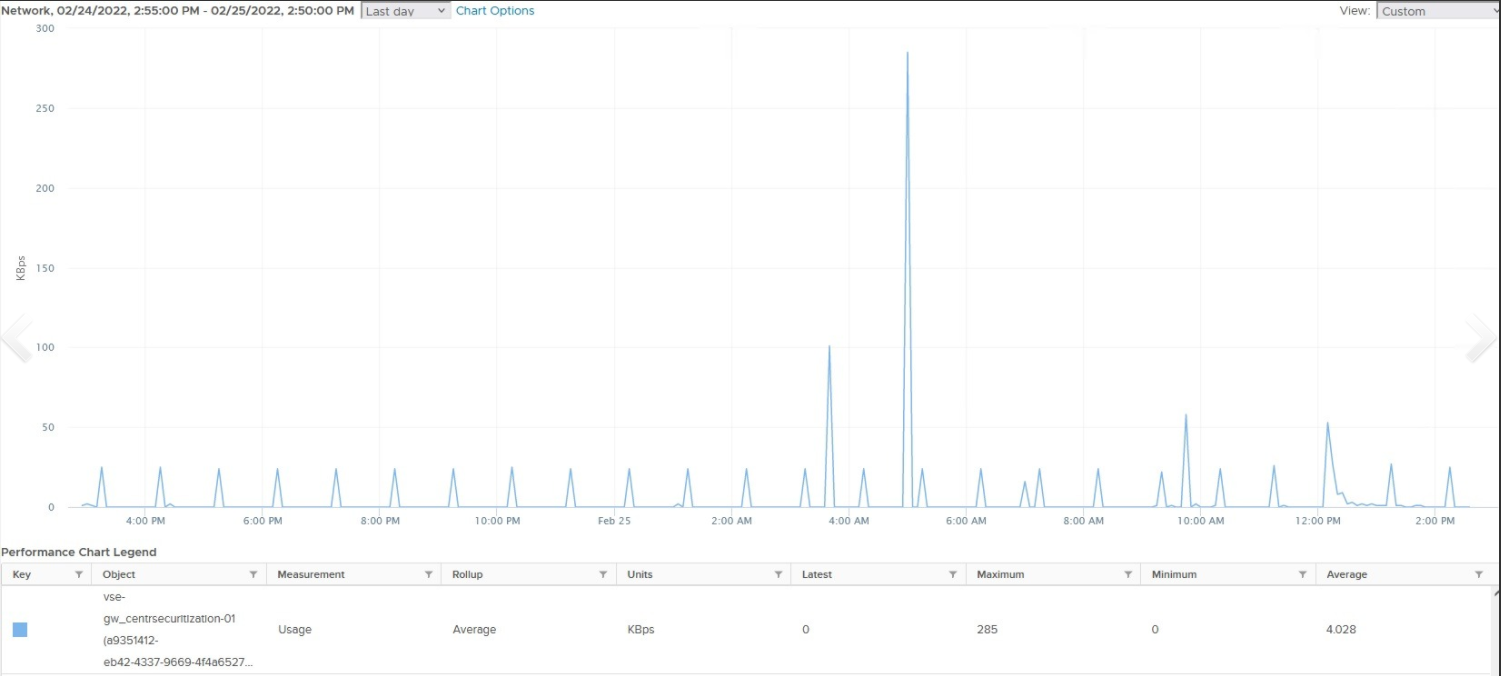


Рисунок 6.2.2 – Контроль за параметрами и правильностью функционирования сетевого оборудования. График утилизации сетевого интерфейса.

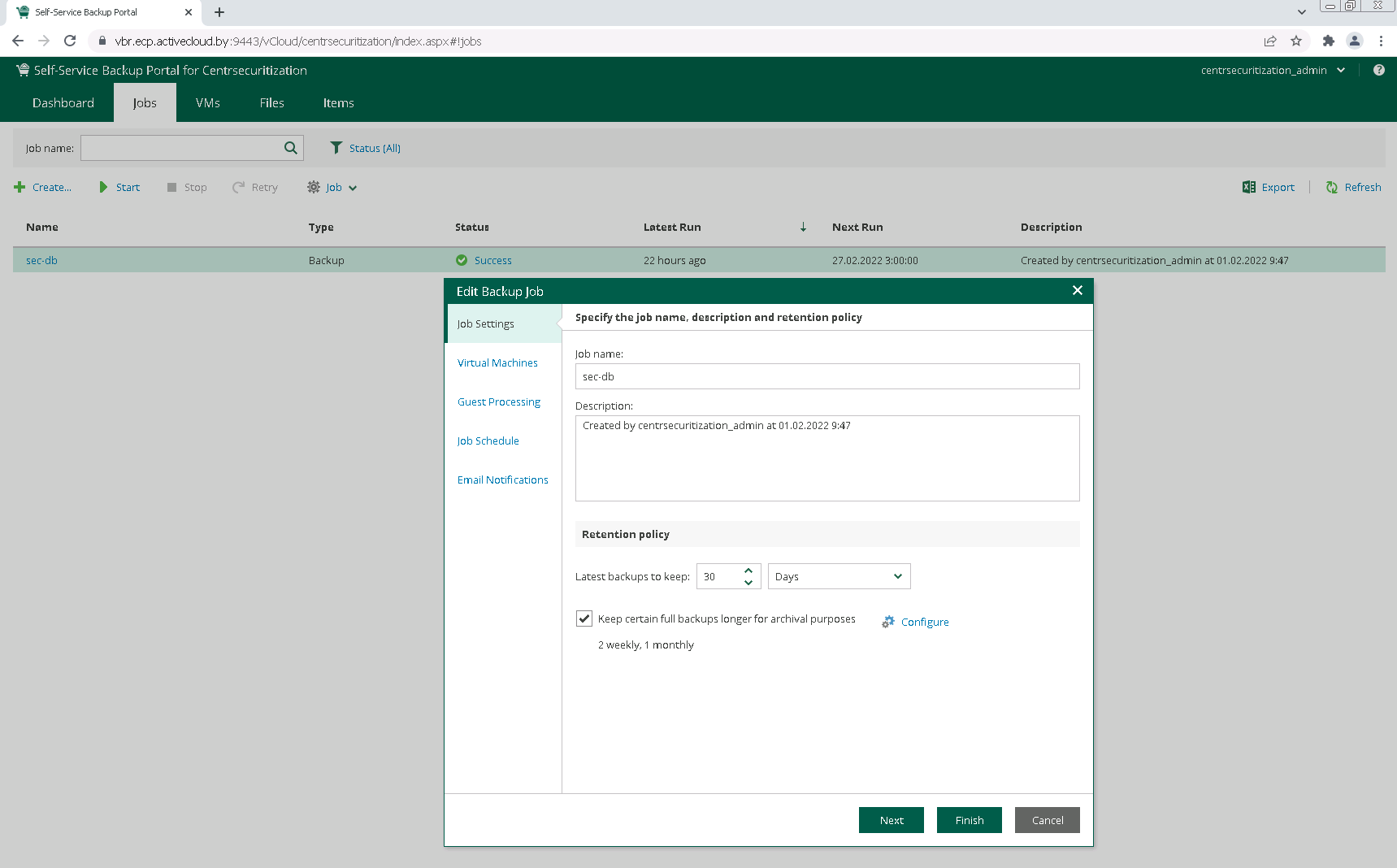


Рисунок 6.2.3 – Настройка доступа к резервным копиям. Интерфейс Veeam Backup.

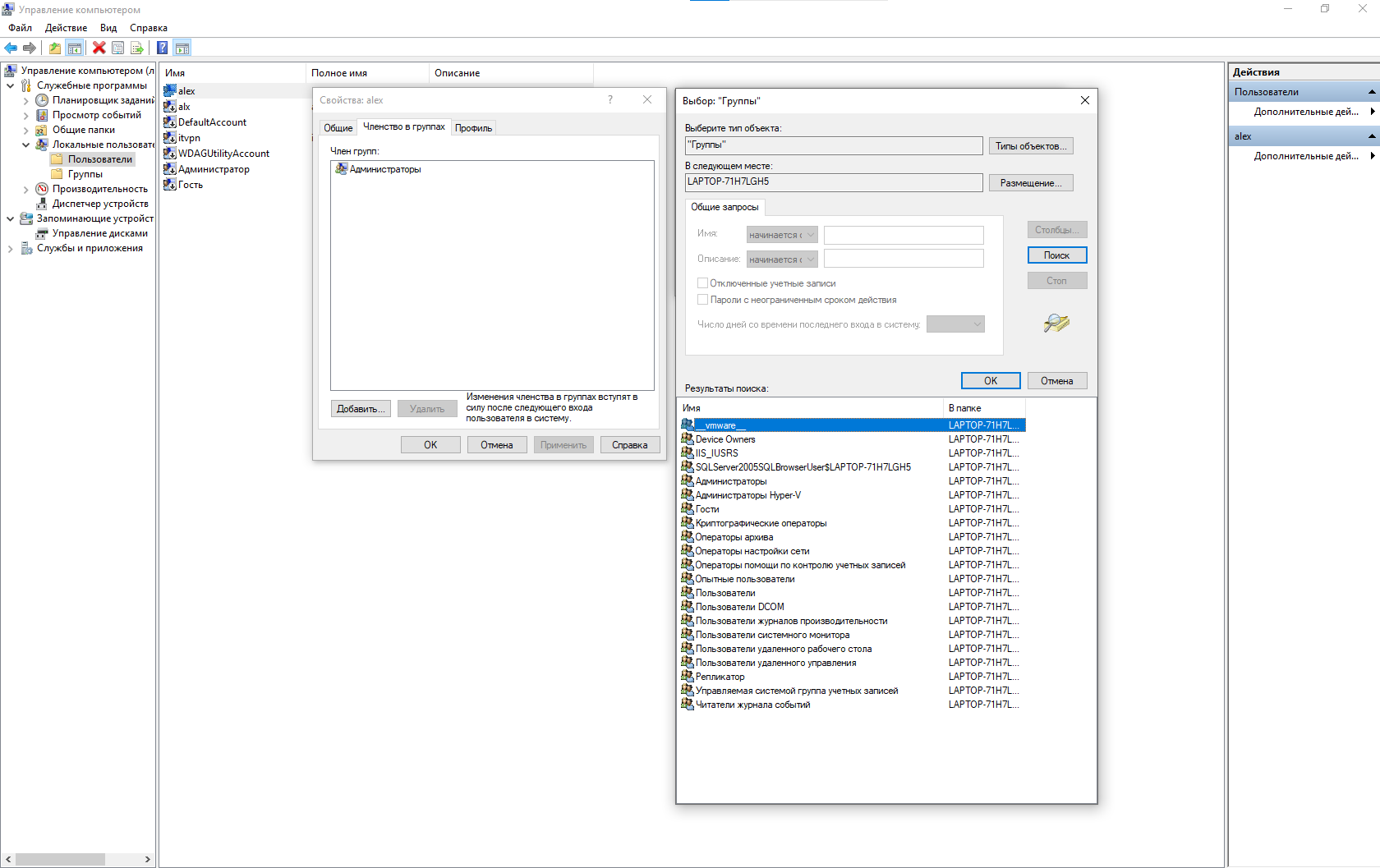


Рисунок 6.2.4 – Настройка доступа к системному программному обеспечению.

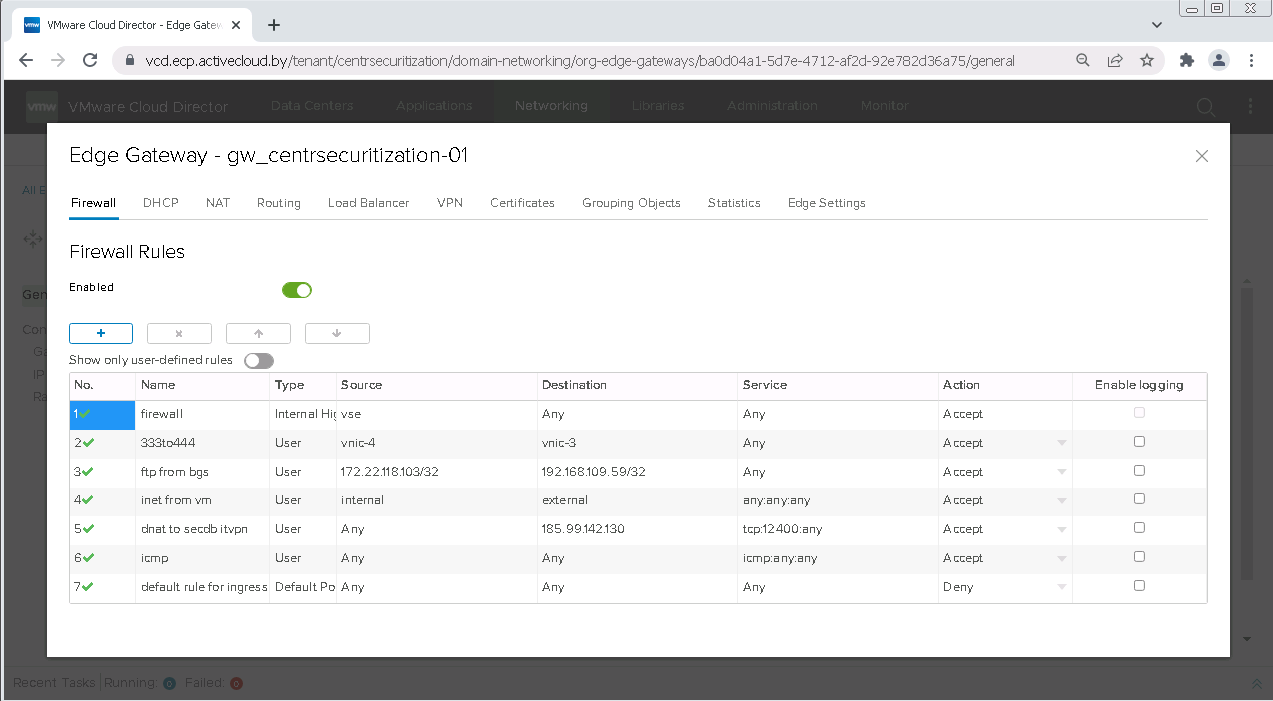


Рисунок 6.2.5 – Настройки сетевого оборудования. Правила межсетевого экранирования gw\_centrsecuritization-01

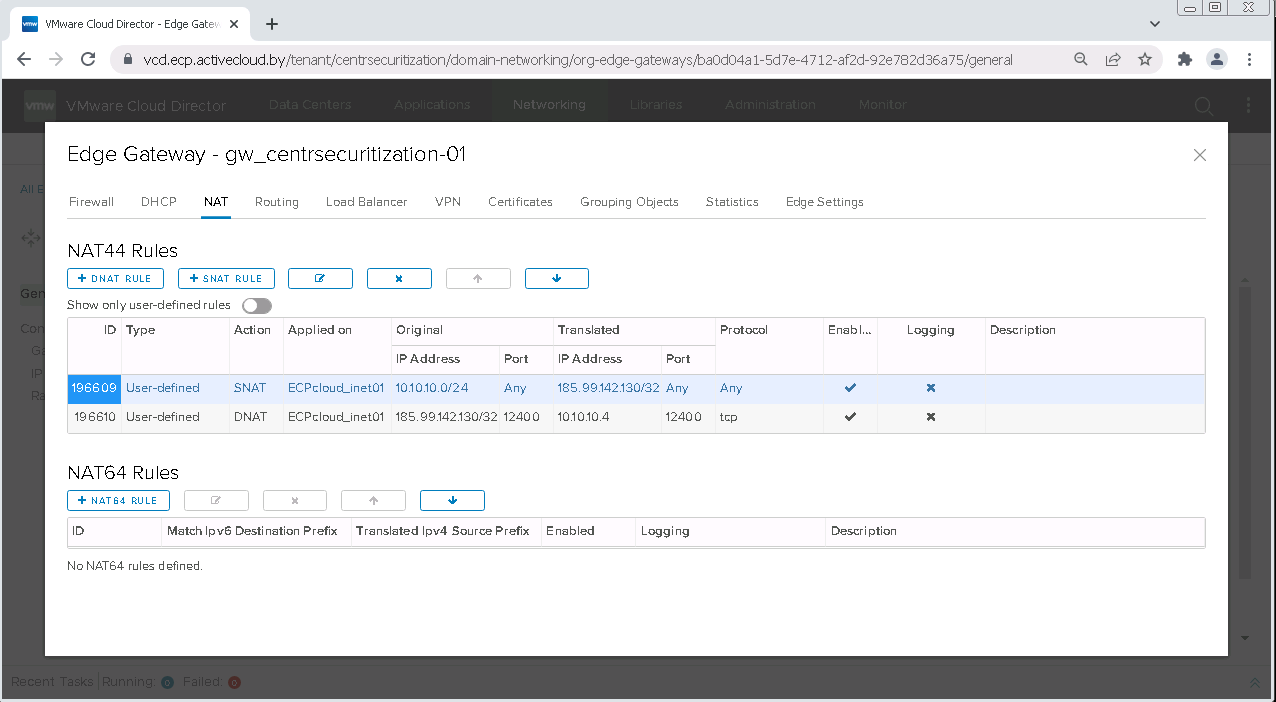


Рисунок 6.2.6 – Настройки сетевого оборудования. Правила трансляции сетевых адресов NAT gw\_ centrsecuritization -01

**УДОСТОВЕРЕНО:**

**Средства программного обеспечения, операционной системы, а также средства технической защиты информации позволяют:**

**контролировать работоспособность, параметры настройки и правильность функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации;**

**обеспечивать защиту от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности.**

контролировать порядок использования в ИС съемных носителей информации, мобильных технических средств – закрыто орг мерами.

**ЗАКЛЮЧЕНИЕ:**

Экспертом удостоверено, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению защиты данных, **соответствуют требованиям**, заявленным в ТЗ.

**6.3. Проверка реализации требований по обеспечению идентификации и аутентификации**

Средства программного обеспечения, операционной системы, а также средства технической защиты информации должны реализовывать:

разграничение доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации;

идентификацию и аутентификацию пользователей ИС;

защиту обратной связи при вводе аутентификационной информации;

полномочное управление (создание, активация, блокировка и уничтожение) учетными записями пользователей ИС;

контроль за соблюдением правил генерации и смены паролей пользователей ИС;

блокировку доступа к объектам ИС после истечения установленного времени бездействия (неактивности) пользователя ИС или по его запросу.

**ПРОЦЕДУРА ТЕСТИРОВАНИЯ:**

Эксперт удостоверяет, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению идентификации и аутентификации, соответствуют требованиям, заявленным в ТЗ.

Ожидаемые результаты тестирования подтверждены и представлены на рисунках 6.1.1 – 6.1.6, 6.3.1 – 6.3.10.

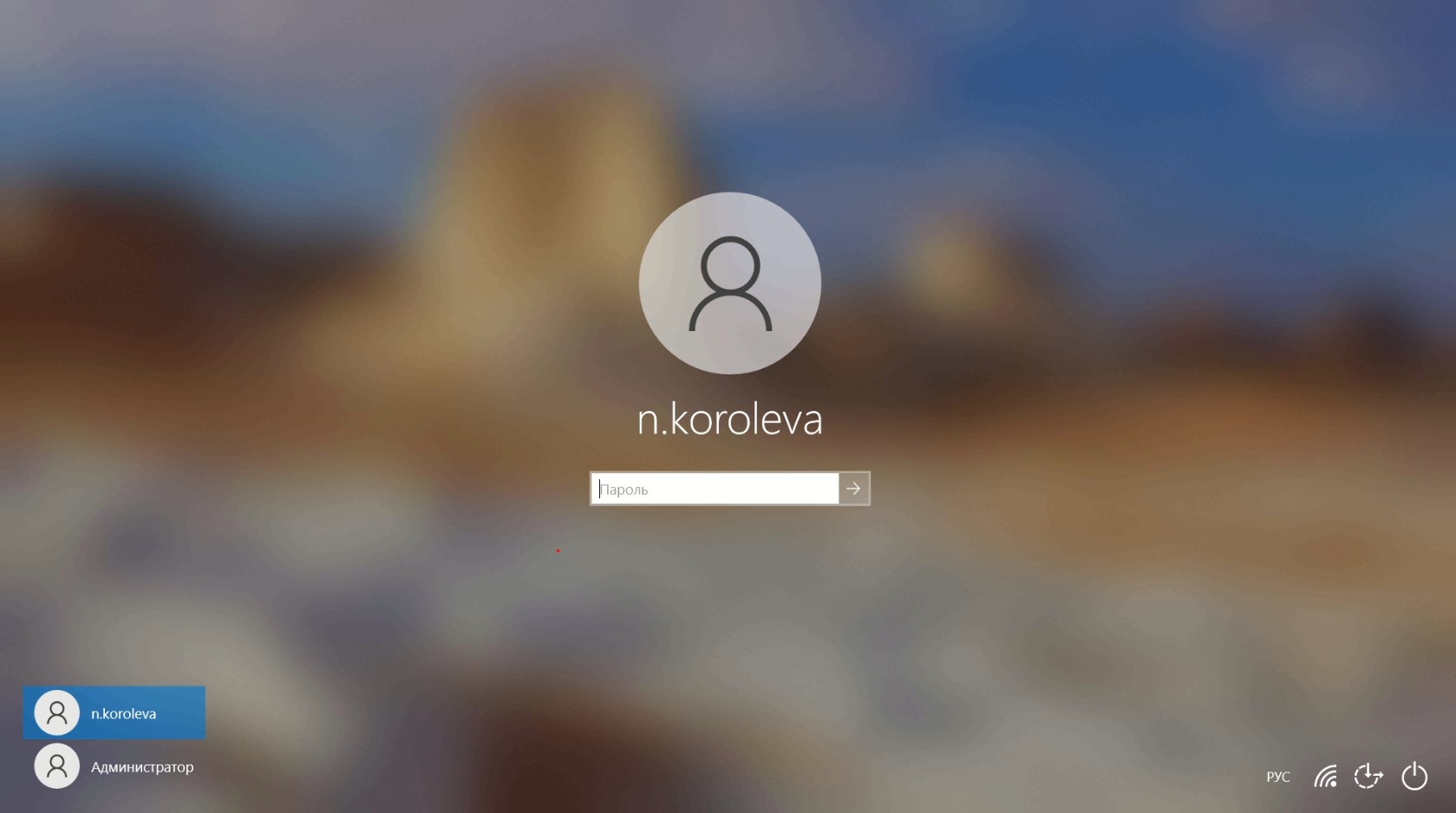


Рисунок 6.3.1 – Вход пользователя в операционную систему

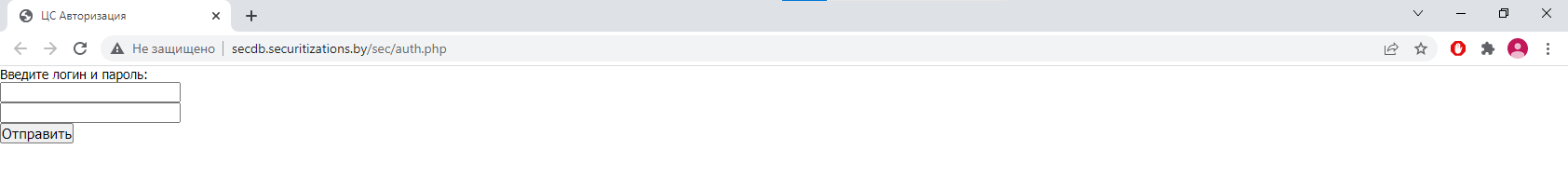


Рисунок 6.3.2 – Вход пользователя в «Учет операций секьюритизации»

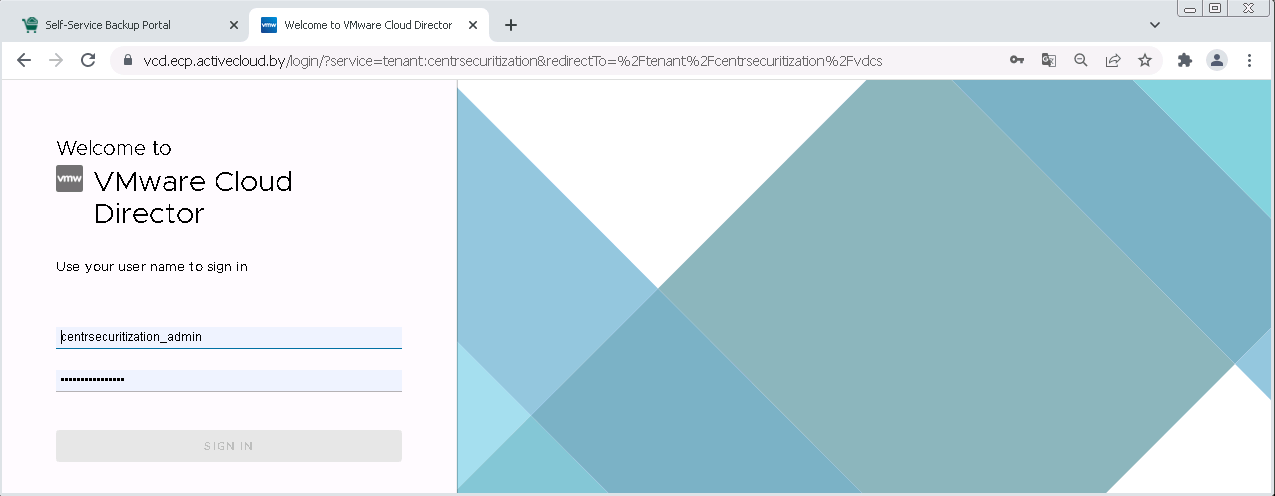


Рисунок 6.3.3 – Вход пользователя в административную панель VMware Cloud Director.

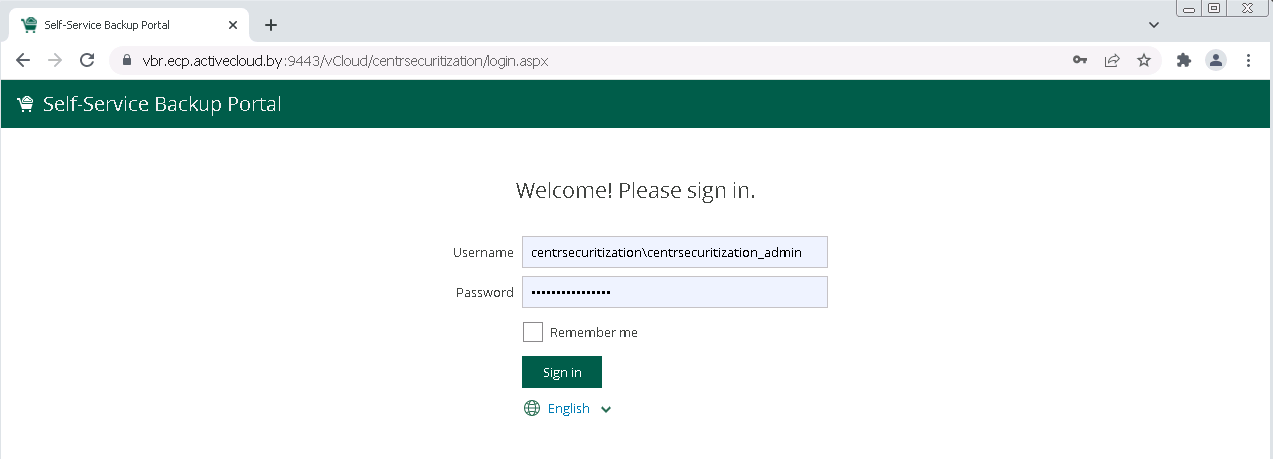


Рисунок 6.3.4 – Вход пользователя в административную панель Veeam Backup and Replication.



Рисунок 6.3.5 – Сертификат соответствия Veeam Backup and Replication версии 9.5.

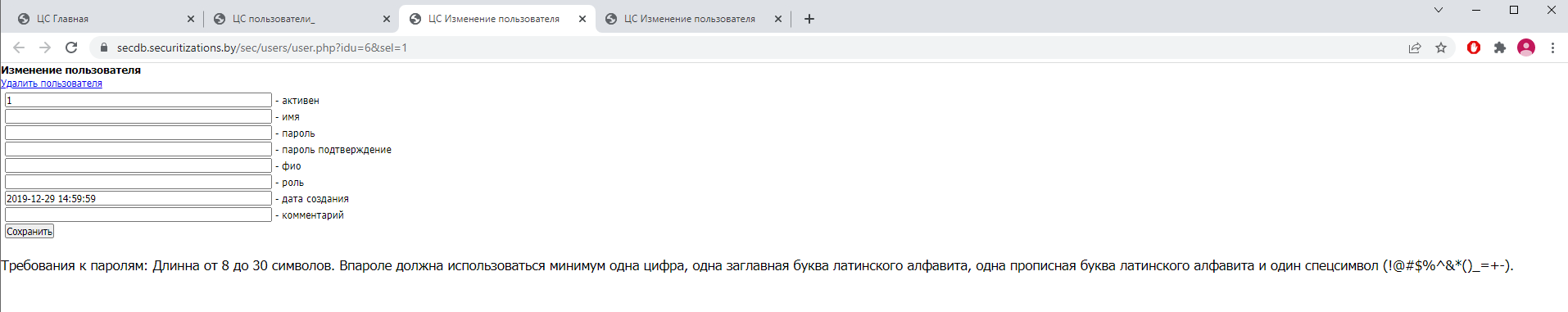


Рисунок 6.3.6 – Управление (создание, активация, блокировка и уничтожение) учетными записями пользователей ИС

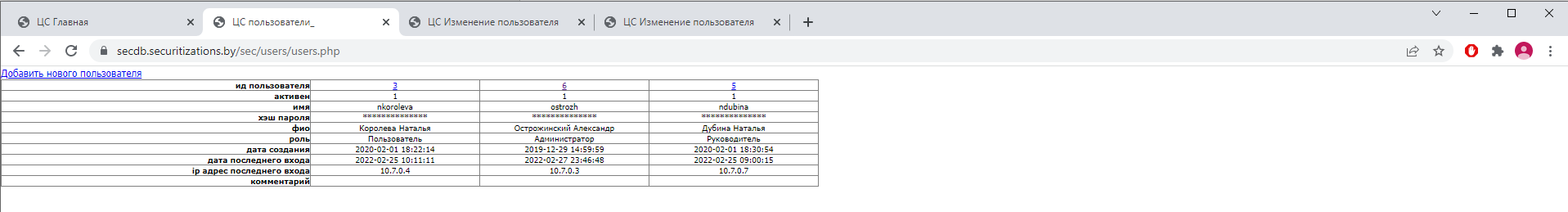


Рисунок 6.3.7 – Управление (создание, активация, блокировка и уничтожение) учетными записями пользователей ИС

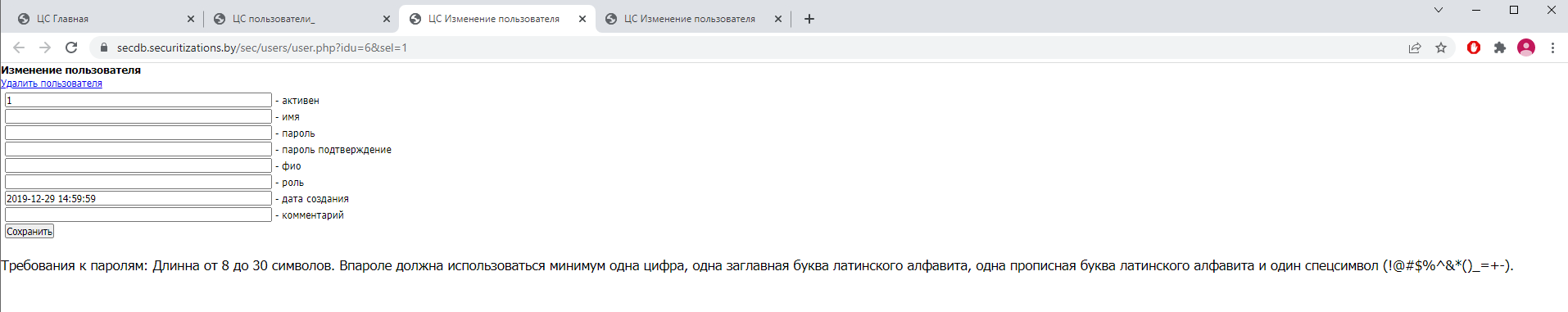


Рисунок 6.3.8 – Настройки требований к паролю в ИС “Учет операций секьюритизации”

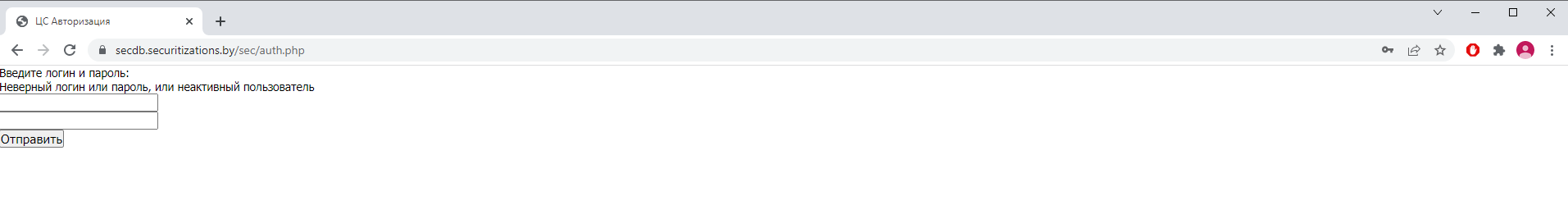


Рисунок 6.3.9 – Блокировка после неудачных попыток входа

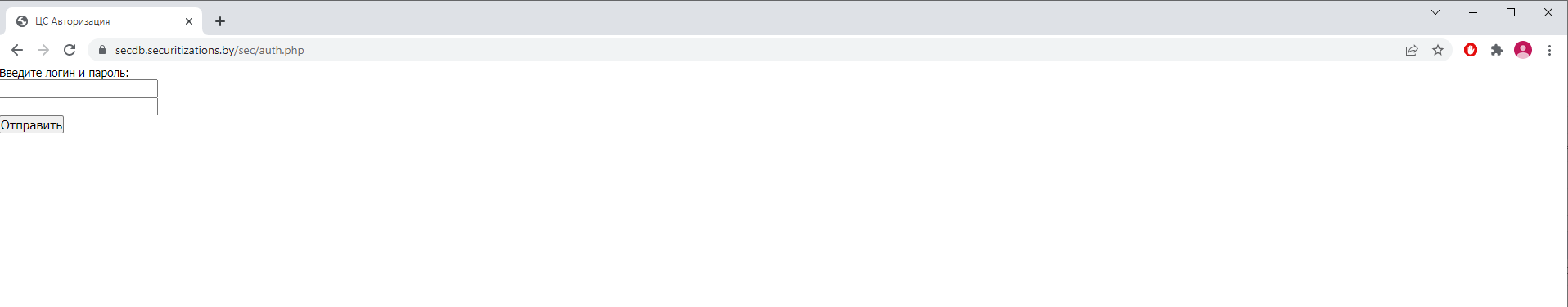


Рисунок 6.3.10 – Блокировка доступа к ИС установленного времени

**УДОСТОВЕРЕНО:**

**Средства программного обеспечения, операционной системы, а также средства технической защиты реализуют:**

**разграничение доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации;**

**идентификацию и аутентификацию пользователей ИС;**

**защиту обратной связи при вводе аутентификационной информации;**

**полномочное управление (создание, активация, блокировка и уничтожение) учетными записями пользователей ИС;**

**контроль за соблюдением правил генерации и смены паролей пользователей ИС;**

**блокировку доступа к объектам ИС после истечения установленного времени бездействия (неактивности) пользователя ИС или по его запросу.**

**ЗАКЛЮЧЕНИЕ:**

Эксперт удостоверено, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению идентификации и аутентификации, **соответствуют требованиям**, заявленным в ТЗ.

**6.4. Проверка реализации требований по обеспечению защиты системы защиты информации ИС**

Средства программного обеспечения, операционной системы, сетевого оборудования, а также средства технической защиты должны обеспечивать:

право уполномоченному пользователю ИС на изменения атрибутов безопасности, установленных по умолчанию в соответствии с политикой информационной безопасности;

возможность обновление объектов информационной системы;

контроль и управление физическим доступом в помещения, в которых постоянно размещаются объекты ИС;

синхронизация временных меток и (или) системного времени в ИС и системе защиты информации.

**ПРОЦЕДУРА ТЕСТИРОВАНИЯ:**

Эксперт удостоверяет, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению защиты системы защиты информации ИС, соответствуют требованиям, заявленным в ТЗ.

Результаты тестирования подтверждены и представлены на рисунках 6.1.1 – 6.1.5, 6.4.1 – 6.4.5.

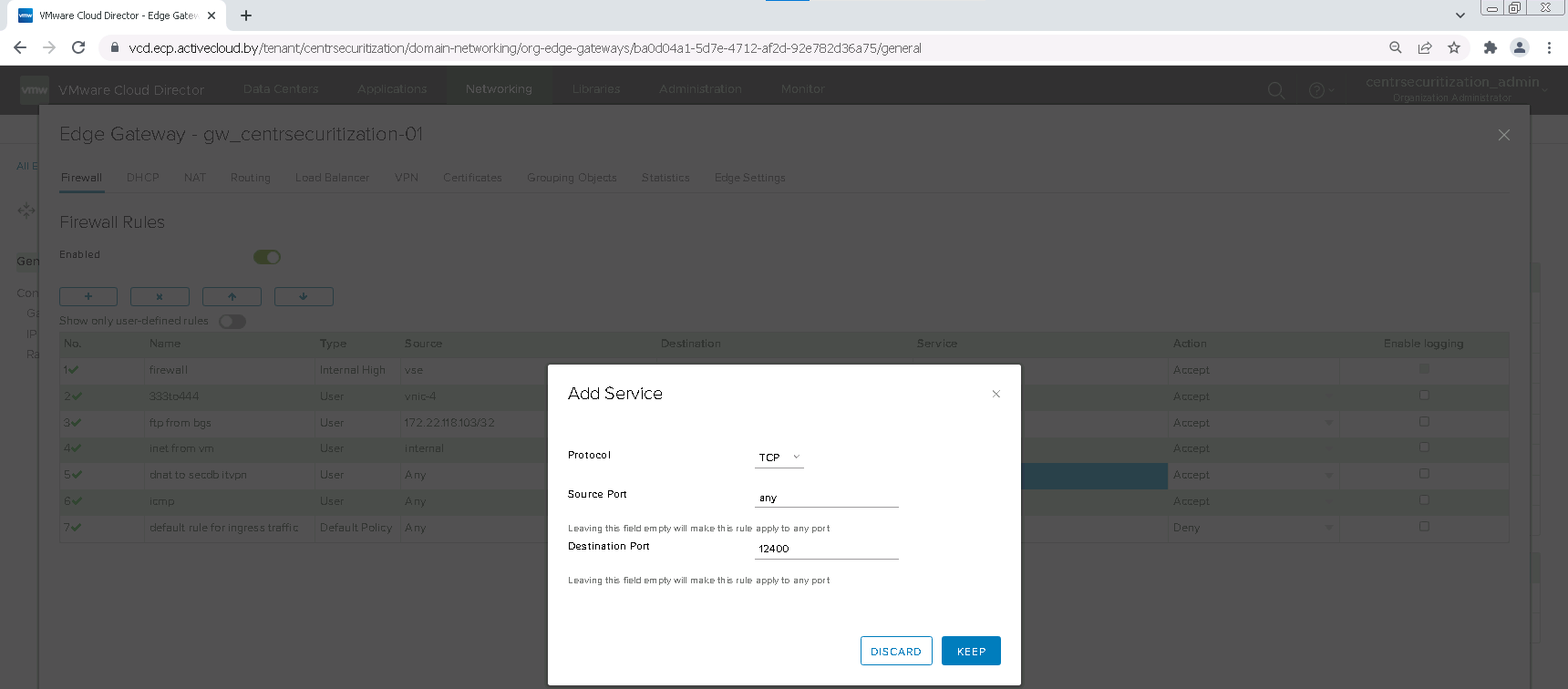


Рисунок 6.4.1 – Изменение атрибутов безопасности сетевого оборудования, установленных по умолчанию.

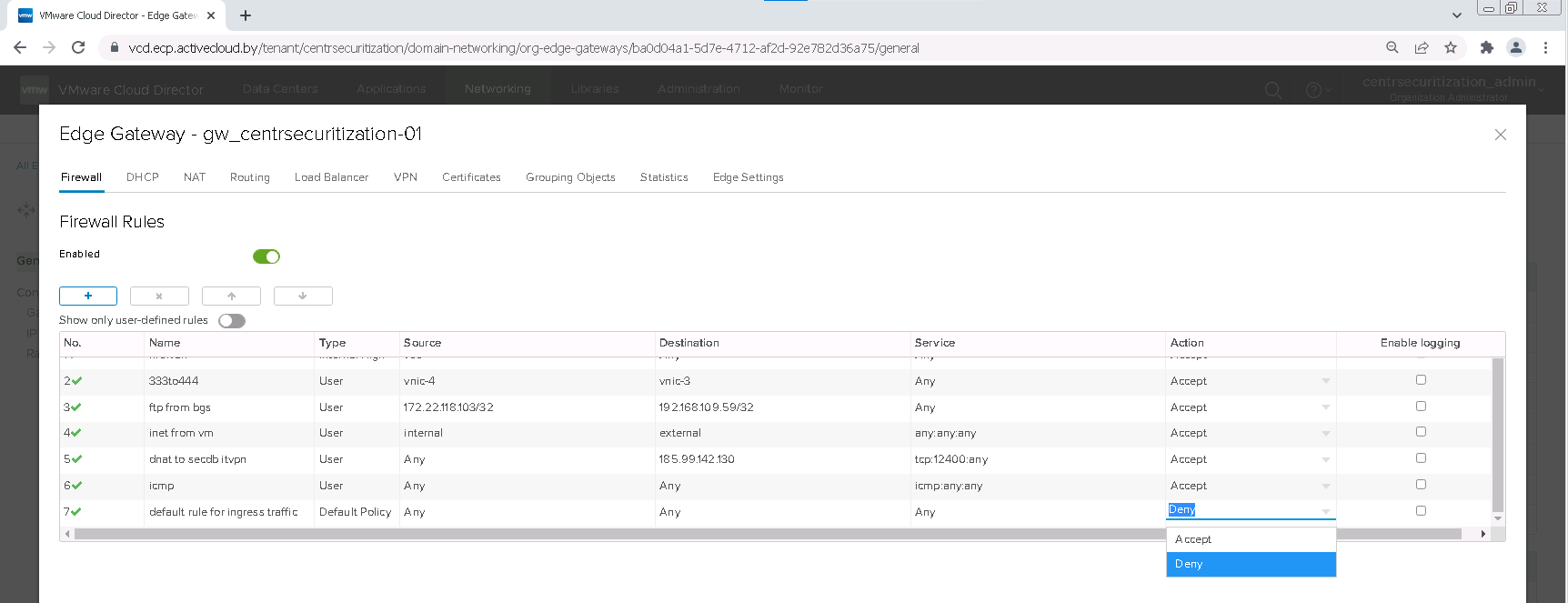


Рисунок 6.4.2 – Изменение правил сетевого оборудования, установленных по умолчанию.

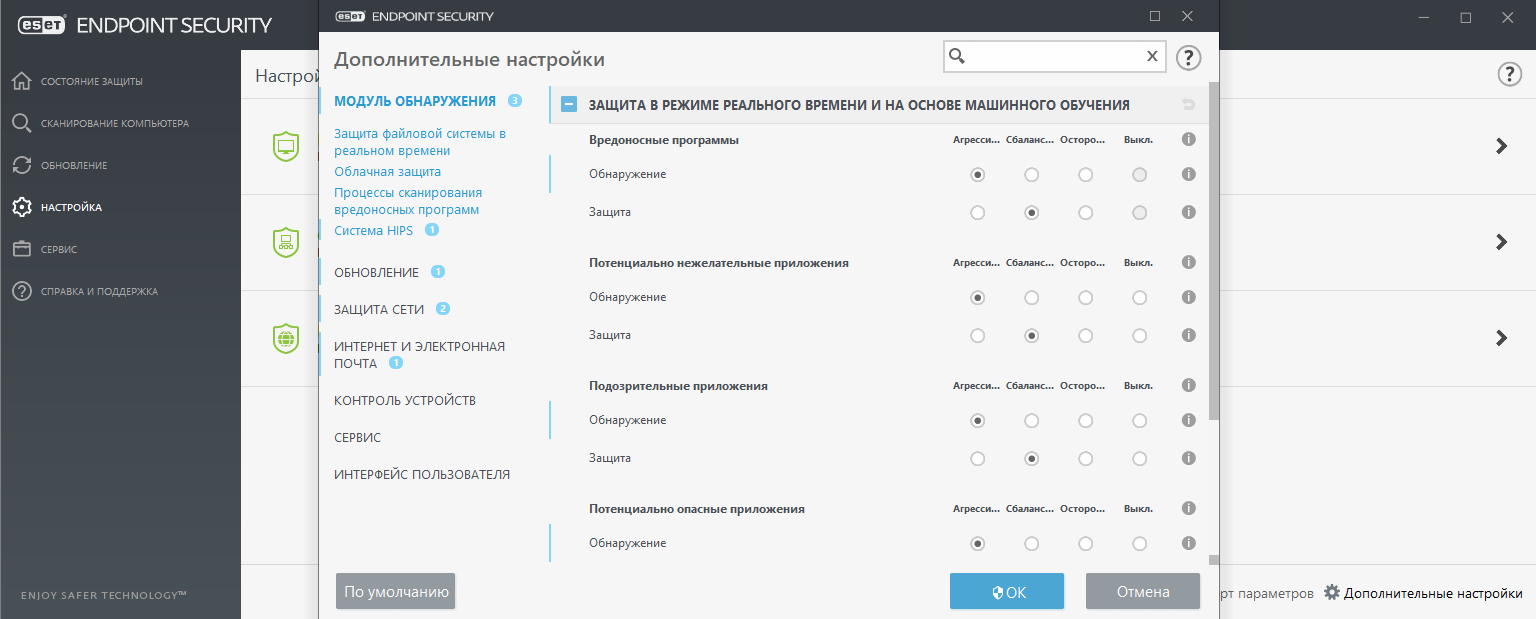


Рисунок 6.4.3 – Измененные атрибуты безопасности средств защиты информации, установленных по умолчанию (антивирусное ПО).

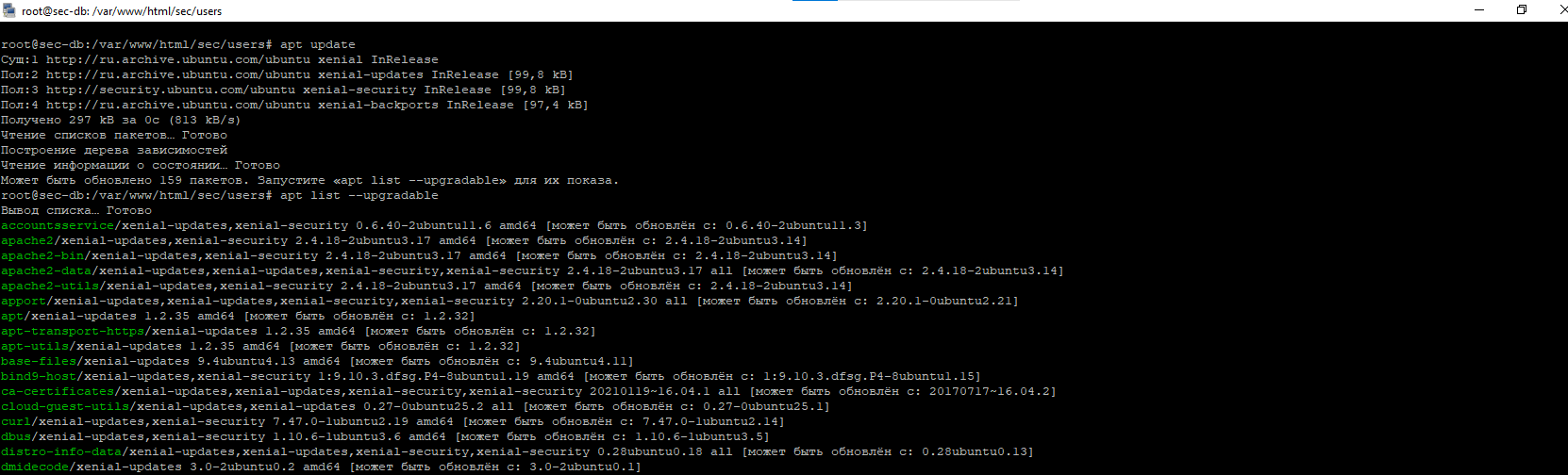


Рисунок 6.4.4 – Доступность обновлений компонентов информационной системы.

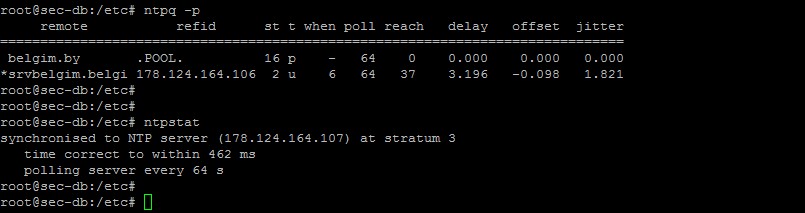


Рисунок 6.4.5 – Настройка синхронизации временных меток и (или) системного времени в ИС и системе защиты информации

**УДОСТОВЕРЕНО:**

**Средства программного обеспечения, операционной системы, сетевого оборудования, а также средства технической защиты обеспечивают:**

**право уполномоченному пользователю ИС на изменения атрибутов безопасности, установленных по умолчанию в соответствии с политикой информационной безопасности;**

**возможность обновление объектов информационной системы;**

**контроль и управление физическим доступом в помещения, в которых постоянно размещаются объекты ИС;**

**синхронизация временных меток и (или) системного времени в ИС и системе защиты информации.**

**ЗАКЛЮЧЕНИЕ:**

Экспертом удостоверено, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению защиты системы защиты информации ИС, **соответствуют требованиям**, заявленным в ТЗ.

**6.5. Проверка реализации требований по обеспечению криптографической защиты информации**

Средствами криптографической защиты информации (средствами контроля целостности) должен обеспечиваться контроль целостности данных в ИС.

**ПРОЦЕДУРА ТЕСТИРОВАНИЯ:**

Эксперт удостоверяет, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению криптографической защиты информации, соответствуют требованиям, заявленным в ТЗ.

Ожидаемые результаты тестирования подтверждены и представлены на рисунке 6.5.1, 6.5.2.

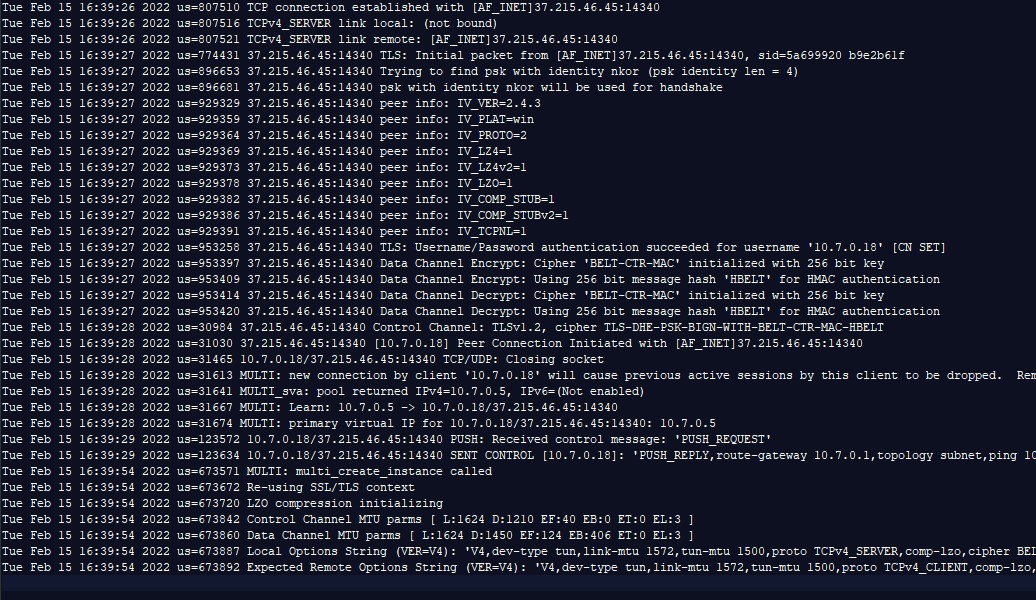
Рисунок 6.5.1 - реализация требований по обеспечению криптографической защиты информации



Рисунок 6.5.2 – Сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь.

**УДОСТОВЕРЕНО:**

**Средствами криптографической защиты информации (средствами контроля целостности) обеспечивается контроль целостности данных в ИС.**

**ЗАКЛЮЧЕНИЕ:**

Экспертом удостоверено, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению криптографической защиты информации, **соответствуют требованиям**, заявленным в ТЗ.

**6.6. Проверка реализации дополнительных требований по обеспечению защиты информации в виртуальной инфраструктуре**

Виртуальная инфраструктура должна обеспечивать:

защиту от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг;

защиту виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин;

безопасное перемещение виртуальных машин и обрабатываемых на них данных;

резервное копирование пользовательских виртуальных машин;

резервирование сетевого оборудования по схеме N+1;

физическую изоляцию сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

**ПРОЦЕДУРА ТЕСТИРОВАНИЯ:**

Эксперт удостоверяет, что в реальных условиях эксплуатации ИС функции безопасности, реализующие дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре, соответствуют требованиям, заявленным в ТЗ.

Результаты тестирования подтверждены и представлены на рисунке 6.6.1, 6.6.2.

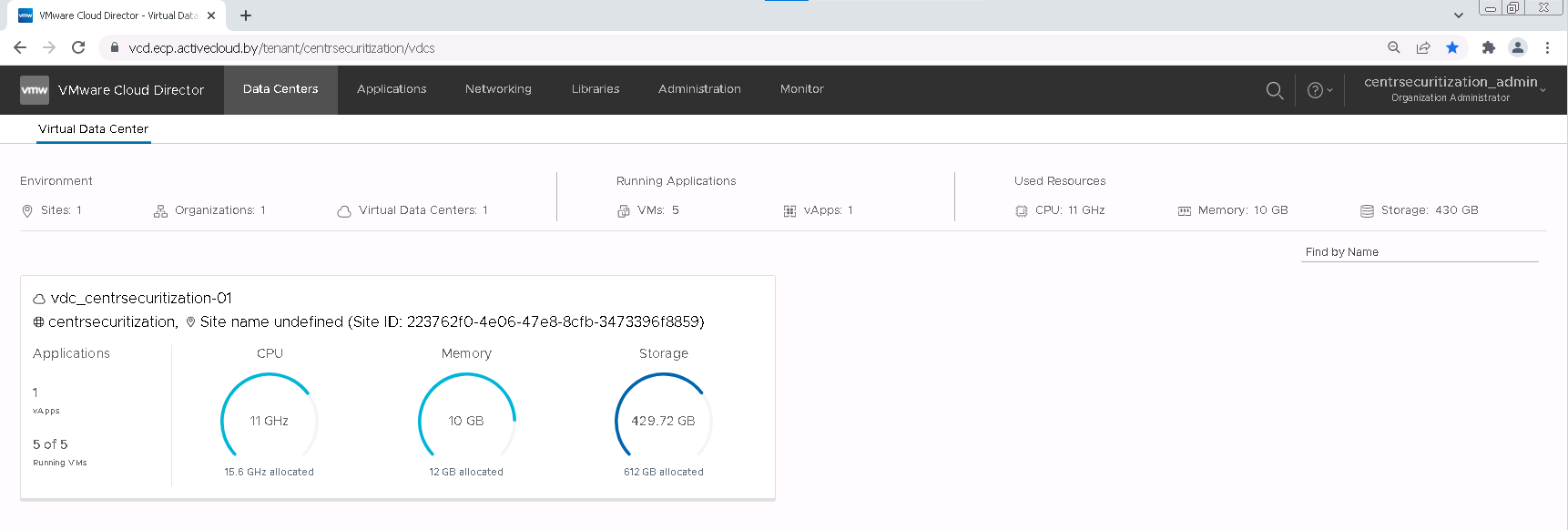


Рисунок 6.6.1 – Защита от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг.

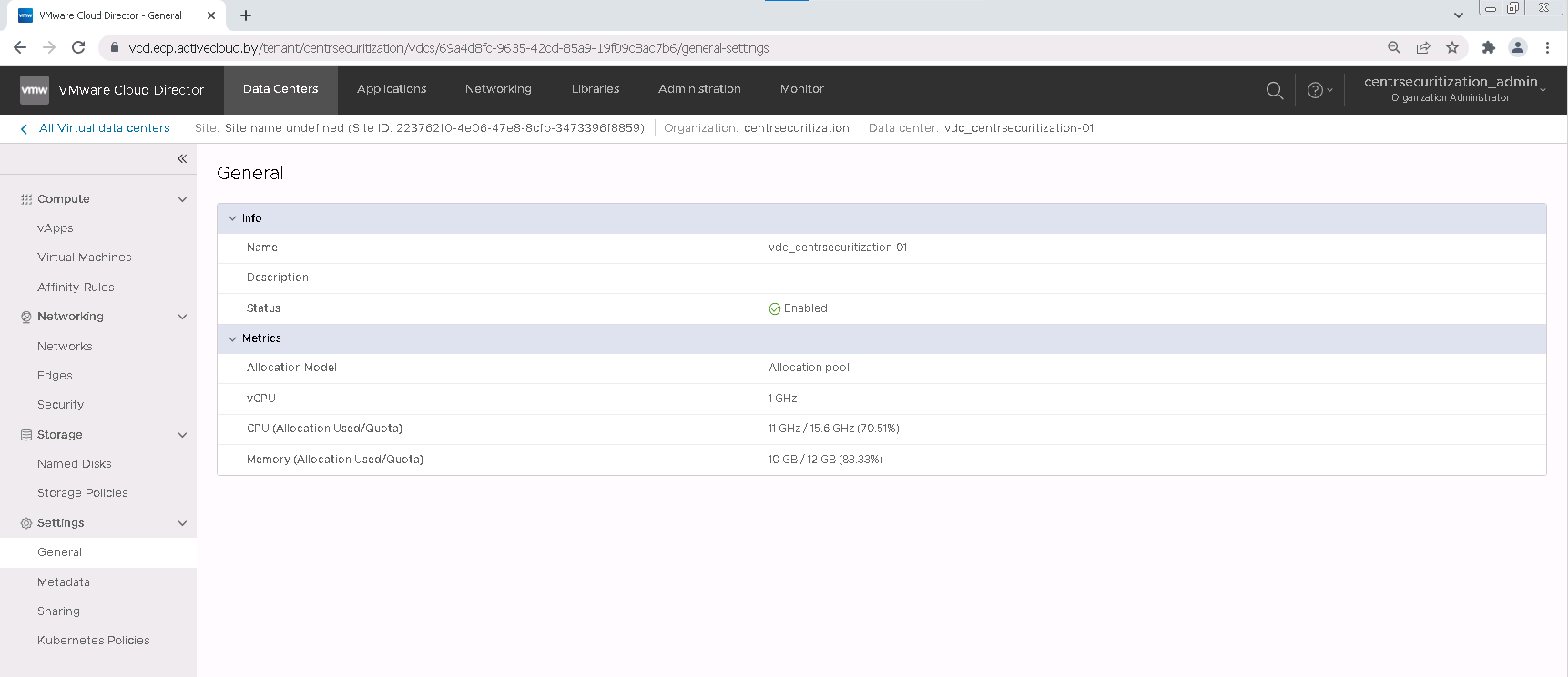


Рисунок 6.6.2 – Защита от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг.

Защита виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин реализована при помощи программно-аппаратного комплекса предотвращения DDoS-атак AntiDDoS8080 серии AntiDDoS8000 с программным обеспечением V500R001, предоставляемого СООО «Белорусские облачные технологии» согласно приложению №2 к Договору №05-ОДк от 1 августа 2015г, а так же с использованием межсетевого экрана Palo Alto VM под управлением программного обеспечения PAN-OS версии 8.0 в среде виртуализации VMware, предоставляемого СООО «Белорусские облачные технологии» согласно приложению №2 к Договору №05-ОДк от 1 августа 2015г.

Резервирование сетевого оборудования по схеме N+1 и физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, реализована на базе платформы E-Cloud Protected, имеющей аттестат соответствия №18 от 31 мая 2019 г.

**УДОСТОВЕРЕНО:**

**Средствами виртуальной инфраструктуры и техническими средствами ИС обеспечивается:**

**защита от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг;**

**защита виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин;**

**безопасное перемещение виртуальных машин и обрабатываемых на них данных;**

**резервное копирование пользовательских виртуальных машин;**

**резервирование сетевого оборудования по схеме N+1;**

**физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.**

**ЗАКЛЮЧЕНИЕ:**

Экспертом удостоверено, что в реальных условиях эксплуатации ИС функции безопасности, реализующие требования по обеспечению дополнительных требований по обеспечению защиты информации в виртуальной инфраструктуре, **соответствуют требованиям**, заявленным в ТЗ.

**6.7. Проверка реализации иных требований**

Средства программного обеспечения, операционной системы, а также средства технической защиты информации должны позволять:

использовать объекты ИС под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов ИС или особенностей объектов ИС);

определять состав и содержания информации, подлежащей резервированию;

резервировать информацию;

обновлять программного обеспечения объектов ИС;

защищать средства вычислительной техники от вредоносных программ.

**ПРОЦЕДУРА ТЕСТИРОВАНИЯ:**

Эксперт удостоверяет, что в реальных условиях эксплуатации ИС функции безопасности, реализующие иные требования, соответствуют требованиям, заявленным в ТЗ.

Результаты тестирования подтверждены и представлены на рисунках 6.7.1 – 6.7.5.

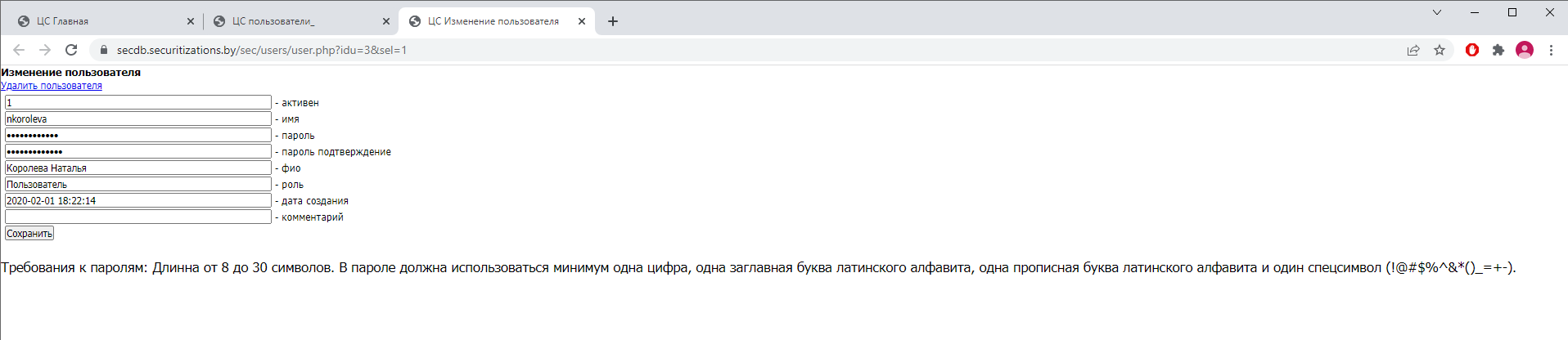


Рисунок 6.7.1 – Настройки пользовательских учетных записей объектов ИС

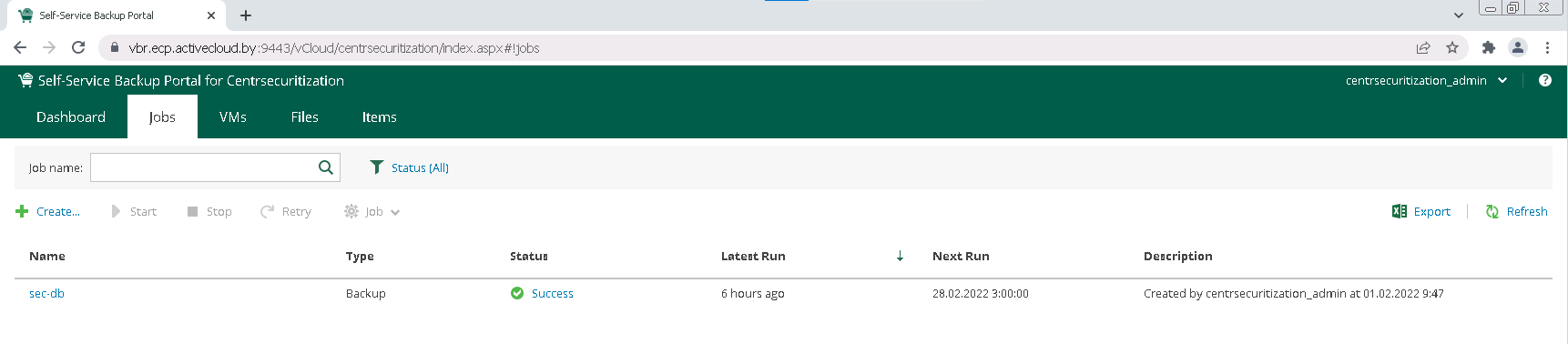


Рисунок 6.7.2 – Настройки состава и содержания информации, подлежащей резервированию

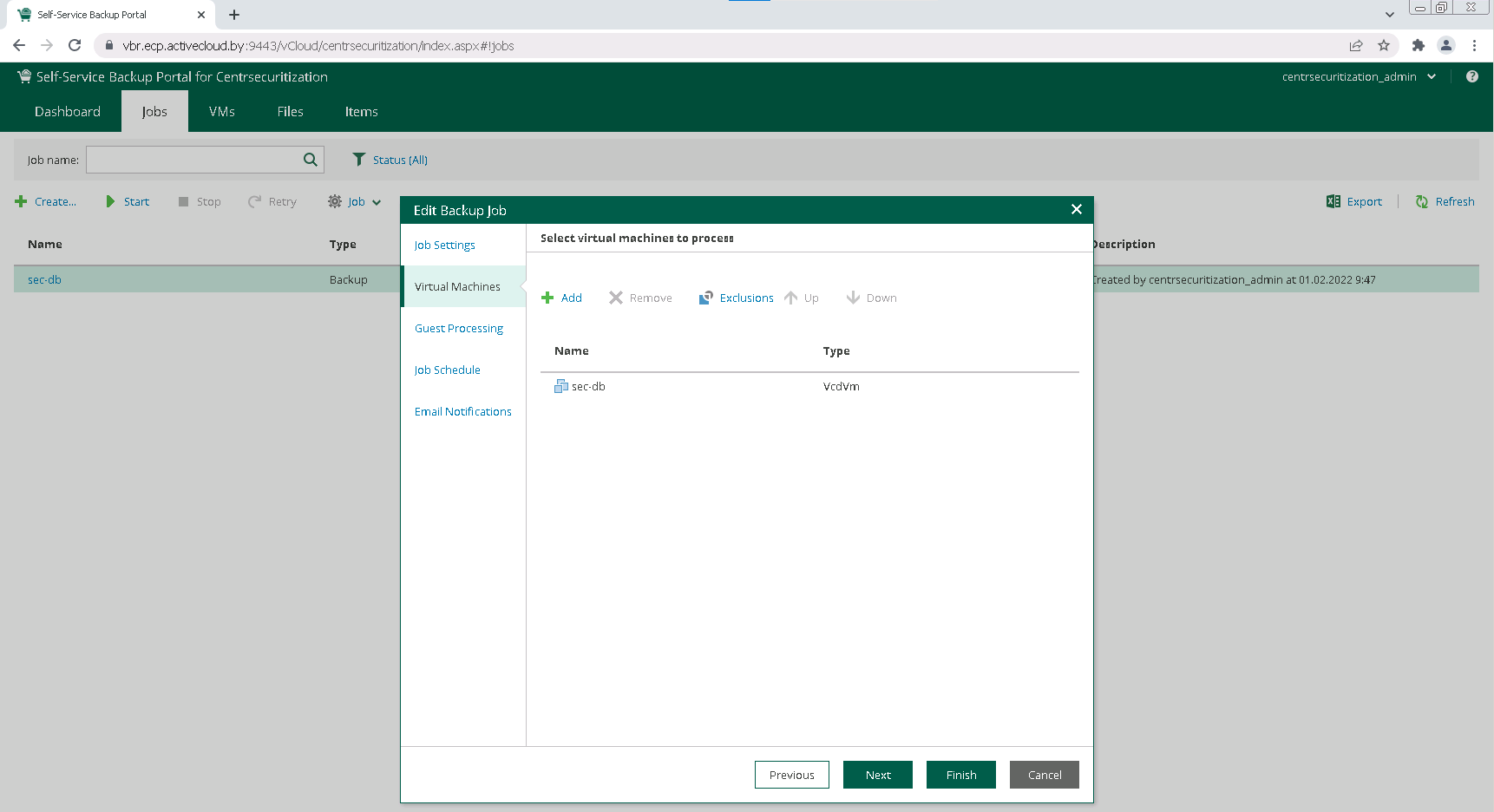


Рисунок 6.7.3 – Настройки по резервированию информации

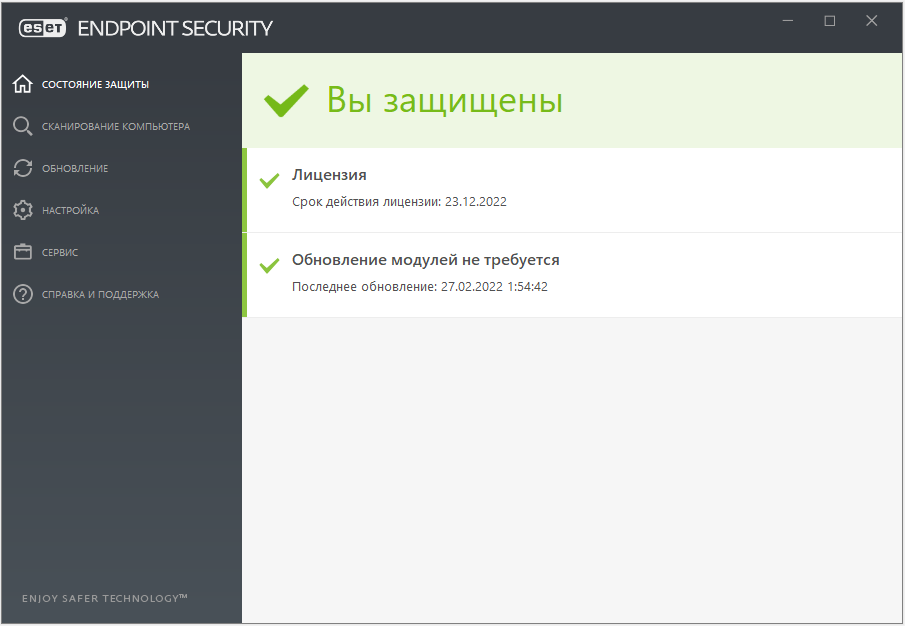


Рисунок 6.7.4 – Установленное средство технической защиты информации (антивирусное средство)

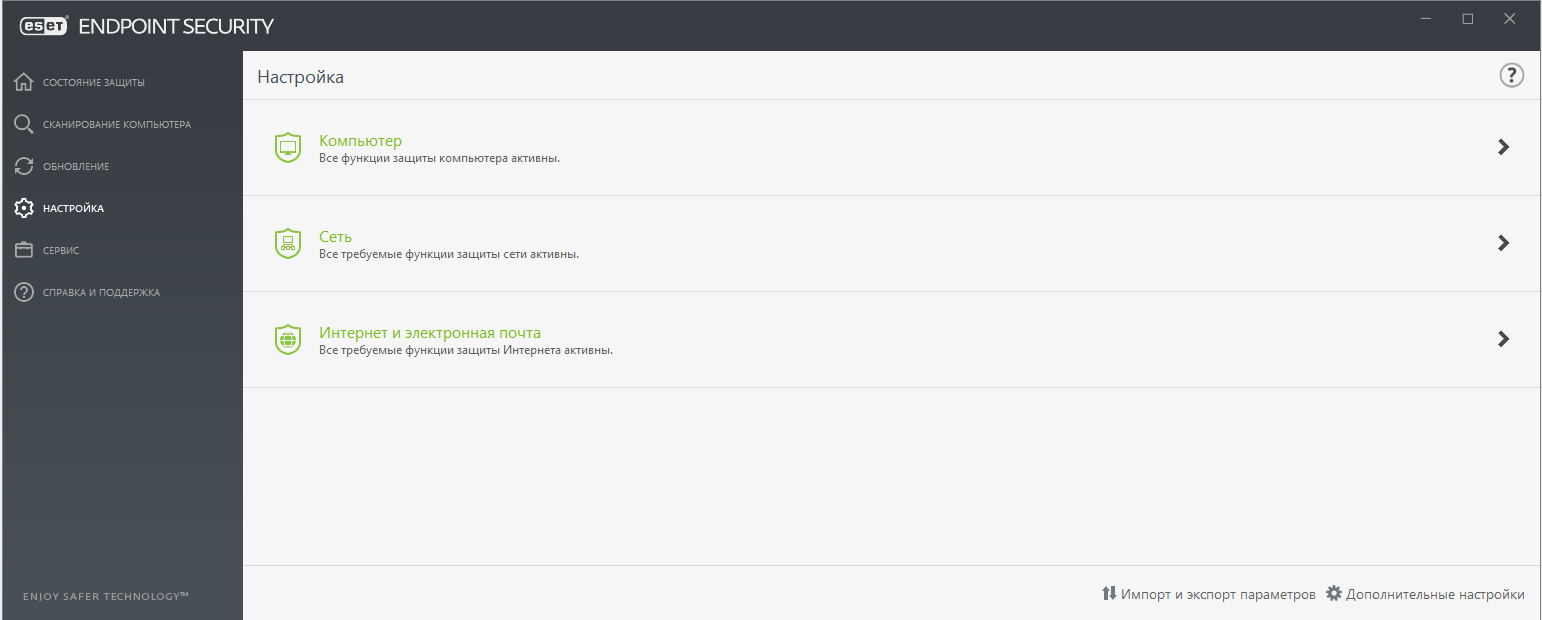


Рисунок 6.7.5 – Настройки средства технической защиты информации (антивирусного средства)

**УДОСТОВЕРЕНО:**

**Средства программного обеспечения, операционной системы, а также средства технической защиты информации позволяют:**

**использовать объекты ИС под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов ИС или особенностей объектов ИС);**

**определять состав и содержания информации, подлежащей резервированию;**

**резервировать информацию;**

**резервирование конфигурационных файлов сетевого оборудования;**

**обновлять программного обеспечения объектов ИС;**

**защищать средства вычислительной техники от вредоносных программ.**

**ЗАКЛЮЧЕНИЕ:**

Экспертом удостоверено, что в реальных условиях эксплуатации ИС функции безопасности, реализующие иные требования, **соответствуют требованиям**, заявленным в ТЗ.

**7. ОТЧЕТ О ВНЕШНЕЙ И ВНУТРЕННЕЙ ПРОВЕРКЕ ОТСУТСТВИЯ ЛИБО НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ НАРУШИТЕЛЕМ СВОЙСТВ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ И АППАРАТНЫХ СРЕДСТВ**

Внутренняя и внешняя проверка отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств ИС, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы была проведена в составе испытаний системы защиты информации на предмет выполнения установленных требований безопасности и корректности функционирования ИС, а также с использованием программного продукта «Сканер уязвимостей Nessus Professional (Tenable.sc)», имеющего Сертификат соответствия Техническому регламенту Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), выданный в Национальной системе подтверждения соответствия Республики Беларусь. Регистрационный номер сертификата - BY/112 02.02.036 01261.

Результаты сканирования от \_\_.03.2022 на наличие уязвимостей ИС с использованием «Сканер уязвимостей Nessus Professional (Tenable.sc)» представлены в виде приложения к техническому отчету.

**Испытания провели:**

|  |  |  |
| --- | --- | --- |
| Ведущий специалист по защите информации ООО «Активные технологии» (секретарь комиссии) | – | Грецкий Антон Владимирович |
| Системный администратор  ЗАО «Специальная финансовая организация «Центр секьюритизации» | – | Острожинский Александр Николаевич |