



**ПРОГРАММНЫЙ КОМПЛЕКС
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ
«НОВЫЕ ТЕХНОЛОГИИ»
Версия: 2.3.3**

Руководство пользователя

RU.33654484.0001-05 90 01

Листов 74

АННОТАЦИЯ

Настоящий документ является руководством пользователя изделия Программный комплекс «Система контроля действий поставщиков ИТ-услуг «Новые Технологии» (далее – СКДПУ НТ).

Данный документ содержит сведения о назначении и условиях применения СКДПУ НТ. Документ содержит описание действий по осуществлению мониторинга деятельности пользователей целевых систем, управлению инцидентами, а также формированию отчетных материалов на основе полученных данных по интересующим целевым системам и их пользователям.

СОДЕРЖАНИЕ

1 Назначение и область применения СКДПУ НТ.....	5
2 Требования к пользователю СКДПУ НТ.....	6
3 Минимальные характеристики аппаратно-программного обеспечения АРМ.....	7
4 Начало работы.....	8
4.1 Вход.....	8
4.2 Описание интерфейса.....	9
4.3 Редактирование учетной записи пользователя СКДПУ НТ.....	11
5 Основы работы.....	13
5.1 Маркировка персон по устойчивым признакам.....	13
6 Мониторинг.....	14
6.1 Самые продолжительные сессии.....	15
6.2 Активность пользователей.....	16
6.3 Инциденты.....	17
6.4 Основные нарушители.....	17
6.5 Основные инциденты.....	18
6.6 Статистика.....	18
6.7 Активные пользователи.....	19
6.8 Активные пользователи под наблюдением.....	19
6.9 Активность целей.....	20
7 Отчеты.....	22
7.1 Общие сведения.....	22
7.2 Отчеты.....	22
7.3 Библиотека отчетов.....	23
7.3.1 Создание отчета.....	24
7.3.2 Редактирование отчета.....	25
7.3.3 Удаление отчета.....	25
7.3.4 Генерирование отчета.....	26
7.4 Кастомизация отчетов.....	26
7.5 История выполнения.....	27
7.5.1 Скачивание отчета.....	28
7.6 Профили выполнения.....	29
7.6.1 Создание профиля выполнения.....	30
7.6.2 Редактирование профиля выполнения.....	31
7.6.3 Удаление профиля выполнения.....	32
8 Персоны.....	33
8.1 Общие сведения.....	33

8.2 Уровень доверия.....	34
8.3 Склеивание персон.....	35
8.4 Забывание персон.....	35
8.5 Цифровой профиль персоны.....	36
8.5.1 Редактирование информации о персоне.....	38
9 Сессии.....	41
9.1 Общие сведения.....	41
9.2 Профиль пользовательской сессии.....	43
10 Инциденты.....	46
10.1 Общие сведения.....	46
10.2 Карточка инцидента.....	48
10.3 Создать инцидент.....	49
10.4 Редактировать инцидент.....	50
10.5 Назначить ответственного за обработку инцидента.....	52
10.6 Закрыть инцидент.....	53
10.7 Настройка правил белого списка инцидентов.....	54
11 Компоненты.....	56
11.1 Общие сведения.....	56
11.2 Шлюзы.....	56
11.3 Цели.....	57
11.4 Адреса клиента.....	59
Приложение А. Описание инцидентов.....	61
Приложение Б. Описание отчетов.....	64
Перечень сокращений.....	70
Перечень рисунков.....	72
Перечень таблиц.....	73

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ СКДПУ ИТ

СКДПУ ИТ является средством обеспечения безопасности информационных технологий и представляет собой комплекс технологий, позволяющих проводить анализ данных пользовательских сессий на предмет обнаружения признаков инцидентов информационной безопасности в информационных системах, где осуществляется контроль действий привилегированных пользователей.

СКДПУ ИТ имеет только программное исполнение. СКДПУ ИТ способствует реализации политики безопасности организации в части управления инцидентами информационной безопасности.

СКДПУ ИТ - устройство в информационной сети с установленным СКДПУ ИТ, который позволяет сотруднику службы информационной безопасности получать, анализировать, контролировать и обрабатывать весь поток событий, проходящий через установленный в организации Шлюз доступа.

Шлюз доступа (шлюз) - компьютер в информационной сети с установленным СКДПУ, который позволяет осуществлять:

- контроль доступа, запись сеансов и наблюдение за действиями привилегированных пользователей;
- мониторинг действий привилегированных пользователей;
- запись сеансов администрирования; вход привилегированных пользователей через единую точку входа.

2 ТРЕБОВАНИЯ К ПОЛЬЗОВАТЕЛЮ СКДПУ НТ

Пользователь СКДПУ НТ должен обладать практическими навыками работы с графическим пользовательским интерфейсом операционной системы, веб-интерфейсами.

3 МИНИМАЛЬНЫЕ ХАРАКТЕРИСТИКИ АППАРАТНО-ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АРМ

Минимальные рекомендуемые характеристики для работы с СКДПУ НТ представлены в таблице 1.

Таблица 1 – Минимальные характеристики аппаратно-программного обеспечения АРМ пользователя СКДПУ НТ

Компонент	Описание
Процессор	Архитектура x86-64 с тактовой частотой 2 ГГц
Оперативная память	6 ГБ
Жесткий диск	20 ГБ
Дисплей	Разрешение экрана при работ с интерфейсом пользователя не менее 1280x720 (при использовании мобильных устройств возможны ограничения по отображению)
Веб-браузер	Mozilla Firefox 96.0 и выше, Google Chrome 97.0.4692.99 и выше, Microsoft Edge 97.0.1072.55 и выше, Opera 82.0.4227.58 и выше, Safari 15.3 и выше. Обеспечивающий поддержку Java Script, стандарта HTTP 1.1, TLS 1.2 и лучше
Клиентское ПО протоколов удаленного доступа	Свободно распространяемый клиент для различных протоколов удаленного доступа, включая RDP, SSH, TELNET, RLOGIN. В качестве таких клиентов могут быть использованы «PuTTY», «WinSCP», «FileZilla»
Пропускная способность канала связи	Не менее 2Мбит/с

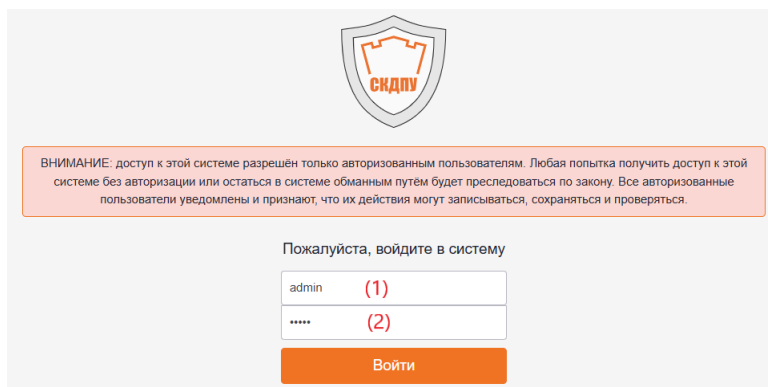
4 НАЧАЛО РАБОТЫ

4.1 Вход

Для получения доступа к графическому веб-интерфейсу СКДПУ НТ необходимо:

Шаг 1. Открыть веб-браузер и в адресной строке ввести адрес сервера СКДПУ НТ.

Шаг 2. В открывшемся окне авторизации следует ввести логин (1) и пароль (2)



Шаг 3. Нажать на кнопку  .



Если для входа пользователя настроена авторизация со вторым фактором, то пользователю будет предложено ввести второй фактор (TOTP-код или пароль от внешнего RADIUS-сервера)

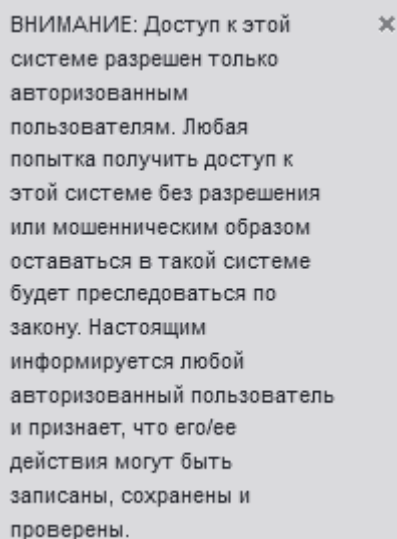
В случае успешной авторизации пользователь переходит в раздел веб-интерфейса СКДПУ НТ.

- выполнен вход в систему



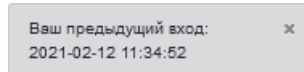
Выполнен вход в систему

- предупреждение пользователя об ответственности неправомерного использования и мерах защиты, реализованных в СКДПУ НТ

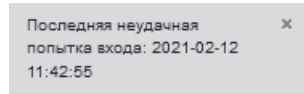


ВНИМАНИЕ: Доступ к этой системе разрешен только авторизованным пользователям. Любая попытка получить доступ к этой системе без разрешения или мошенническим образом оставаться в такой системе будет преследоваться по закону. Настоящим информируется любой авторизованный пользователь и признает, что его/ее действия могут быть записаны, сохранены и проверены.

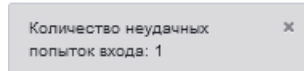
- дата и время предыдущей успешной авторизации



- дата и время последней неудачной авторизации



- количество неудачных попыток авторизации (указывается количество неудачных попыток авторизации, совершенных пользователем до успешной авторизации)



В случае неправильно введенного логина или пароля будет выведено соответствующее сообщение

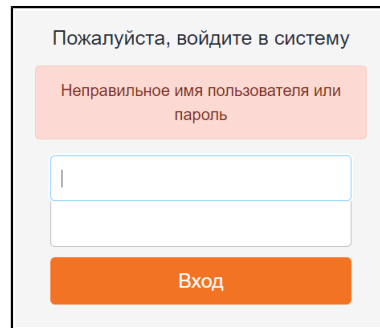


Рисунок 1 – Ошибка входа

4.2 Описание интерфейса

После успешного прохождения процесса идентификации и аутентификации загружается основной интерфейс. Состав основного меню и стартовый раздел интерфейса зависит от настройки доступа для данного пользователя (см. [рисунок 2](#)).

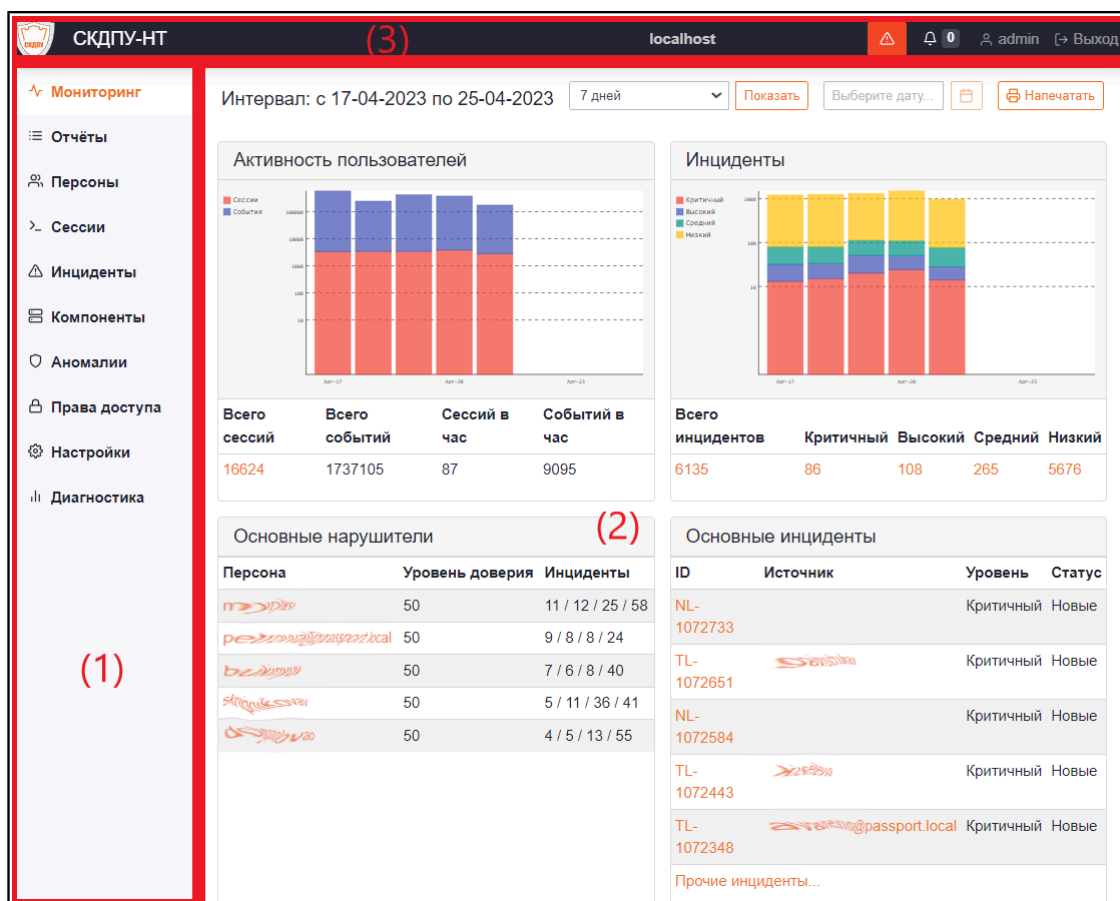
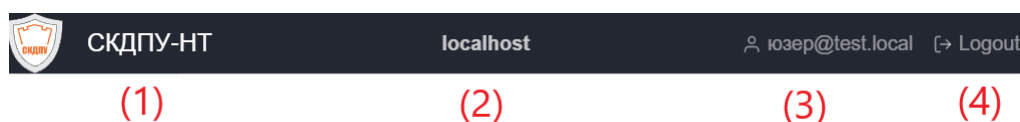


Рисунок 2 – Интерфейс СКДПУ НТ


- (1) – область доступных для текущего пользователя разделов;
- (2) – основная область, где отображается содержимое активного раздела (на рисунке 2 активным разделом является **Мониторинг**);
- (3) – область рассмотрена далее:




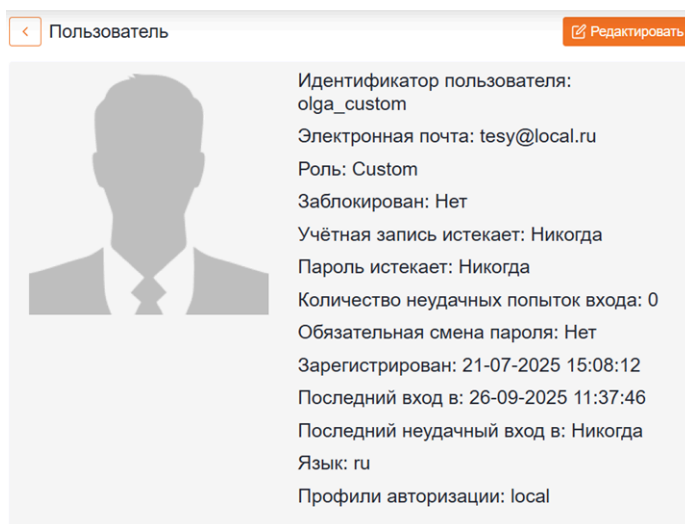
- (1) – логотип и название СКДПУ НТ. При нажатии происходит переход в раздел **Мониторинг**;
- (2) – имя текущего узла. При наведении на него во всплывающей подсказке отображается дополнительно идентификатор узла, его IP-адрес и описание;
- (3) – идентификатор текущего пользователя СКДПУ НТ. При нажатии происходит переход в учетную запись пользователя СКДПУ НТ, где можно редактировать его данные и настройки (см. раздел 4.3);
- (4) – кнопка выхода. При нажатии происходит окончание сессии текущего пользователя СКДПУ НТ.

4.3 Редактирование учетной записи пользователя СКДПУ НТ

Пользователь может изменить свои данные, электронную почту, язык интерфейса и пароль:

Шаг 1. Выбрать профиль пользователя , где **User** – идентификатор текущего пользователя.

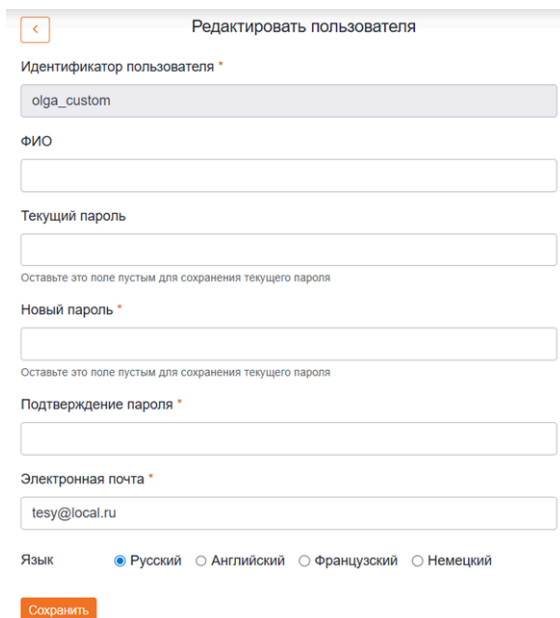
Шаг 2. В открывшейся форме приводятся данные о пользователе, статистика попыток авторизации, сведения о пароле. Далее необходимо нажать на кнопку 



Скриншот интерфейса отображения профиля пользователя. Вверху слева находится кнопка «<» и заголовок «Пользователь». Вверху справа — кнопка «Редактировать». Слева от списка данных — иконка пользователя. Справа — список параметров:

- Идентификатор пользователя: olga_custom
- Электронная почта: tesy@local.ru
- Роль: Custom
- Заблокирован: Нет
- Учётная запись истекает: Никогда
- Пароль истекает: Никогда
- Количество неудачных попыток входа: 0
- Обязательная смена пароля: Нет
- Зарегистрирован: 21-07-2025 15:08:12
- Последний вход в: 26-09-2025 11:37:46
- Последний неудачный вход в: Никогда
- Язык: ru
- Профили авторизации: local

Шаг 3. В появившейся форме изменить желаемые данные



Скриншот интерфейса редактирования профиля пользователя. Вверху — кнопка «<» и заголовок «Редактировать пользователя». Поля для ввода:

- Идентификатор пользователя * (значение: olga_custom)
- ФИО
- Текущий пароль (подсказка: Оставьте это поле пустым для сохранения текущего пароля)
- Новый пароль * (подсказка: Оставьте это поле пустым для сохранения текущего пароля)
- Подтверждение пароля *
- Электронная почта * (значение: tesy@local.ru)

Язык: Русский Английский Французский Немецкий

Внизу — кнопка «Сохранить».


- (1) – ФИО пользователя;
- (2) – текущий пароль учетной записи пользователя;
- (3) – новый пароль учетной записи пользователя;
- (4) – подтверждение нового пароля учетной записи пользователя;
- (5) – адрес электронной почты пользователя;
- (6) – язык веб-интерфейса СКДПУ НТ;



В случае, если нет необходимости в смене пароля, то поля о новом пароле следует оставить незаполненными.

Шаг 4. Сохранить изменения учетной записи нажатием на кнопку 

При успешном сохранении учетной записи появится оповещение

Обновление профиля
пользователя 

5 ОСНОВЫ РАБОТЫ

5.1 Маркировка персон по устойчивым признакам

Подсистема Мониторинг и аналитика автономно выполняет процесс идентификации и классификации пользователей (персон). На основе анализа данных, собранных во время вторичных подключений, подсистема выявляет ключевые характеристики (признаки) и присваивает персонам соответствующие маркеры (теги).

Персоны, промаркированные таким образом, могут быть сгруппированы по выделенным общим признакам (тегам). Отметки (теги) могут выступать как дополнительный критерий фильтрации при работе с профилями персон.

Подсистема предоставляет возможность офицеру безопасности отобрать персоны с похожим поведением, используя механизм поиска на основе тегов.


Поддерживается автоматическое определение следующих характеристик:

Определение преимущественных сервисов работы:

- Персона использует только SSH-сервисы
- Персона использует только RDP-сервисы
- Персона использует преимущественно SSH-сервисы
- Персона использует преимущественно RDP-сервисы

Определение преимущественного времени работы:

- Персона работает преимущественно утром
- Персона работает преимущественно вечером
- Персона работает преимущественно днем
- Персона работает преимущественно ночью
- Использование средств автоматизации действий
- Частая передача файлов-документов

Теги, определенные для профиля персоны, могут быть просмотрены в карточке персоны (см. [раздел 8.5](#)). Офицер безопасности может отфильтровать персоны с похожими характеристиками в карточке персоны (см. [раздел 8.5](#)) или в разделе **Персоны**, задав параметры в поле **Характеристики работы персоны** и нажав на кнопку  (см. [раздел 8](#)).

6 МОНИТОРИНГ

СКДПУ НТ предоставляет возможность оперативного мониторинга деятельности пользователей целевых систем за выбранный промежуток времени в разделе **Мониторинг**.

Предоставляется оперативная информация о пользовательских сессиях и обнаруженных инцидентах в целевых системах, находящихся под контролем, за определенный временной промежуток (1) (см. [рисунок 3](#)).



Рисунок 3 – Раздел **Мониторинг**

Оператор имеет возможность получить статистические данные за определенный временной промежуток в соответствии с выбранными значениями в (2) или за конкретный день(3).

Для выбора доступны следующие временные промежутки (2):

- за текущий день;
- за предыдущий день;
- за последние семь дней;

- за последний период в тридцать один день.

Подтверждение осуществляется нажатием на кнопку [Показать](#).

Также оператор имеет возможность выбрать для просмотра конкретную дату, указав ее в (3) и впоследствии подтвердив нажатием на кнопку [☑](#).

Оператор может оперативно напечатать сводную статистику (4) за выбранный ранее временной промежуток, нажав на кнопку [🖨️ Напечатать](#).

При наличии прав на просмотр оператор СКДПУ НТ имеет возможность перейти в соответствующие разделы для более подробного анализа данных, нажав на активные ссылки, выделенные цветом.

В рассматриваемом разделе представлены статистические данные, выделенные в следующие группы.

6.1 Самые продолжительные сессии

Самые продолжительные сессии			
Персона	Протокол	Сессия	Продолжительность
ploshkoav	SSH	root @ 10.126.168.98	17:07:41
ploshkoav	SSH	root @ 10.126.168.95	15:40:11
ageeys	RDP	asv @ 10.19.102.114	11:12:17
procenkoaa	RDP	a.protsenko @ 172.24.253.179	10:10:32
procenkoaa	RDP	a.protsenko @ 172.24.251.64	9:56:16

Рисунок 4 – Самые продолжительные сессии

В данной группе представлены пять самых продолжительных сессий на целевых системах за выбранный временной промежуток. Здесь указаны персона, инициировавшая сессию, протокол соединения, идентификатор сессии, а также ее продолжительность. Сортировка в таблице по убыванию продолжительности

Пользователь СКДПУ НТ имеет возможность перейти в профили персон, осуществивших доступ к целевым системам (см. [раздел 8](#)), а также просмотреть данные соответствующей сессии подключения к целевой системе (см. [раздел 9](#)).

6.2 Активность пользователей

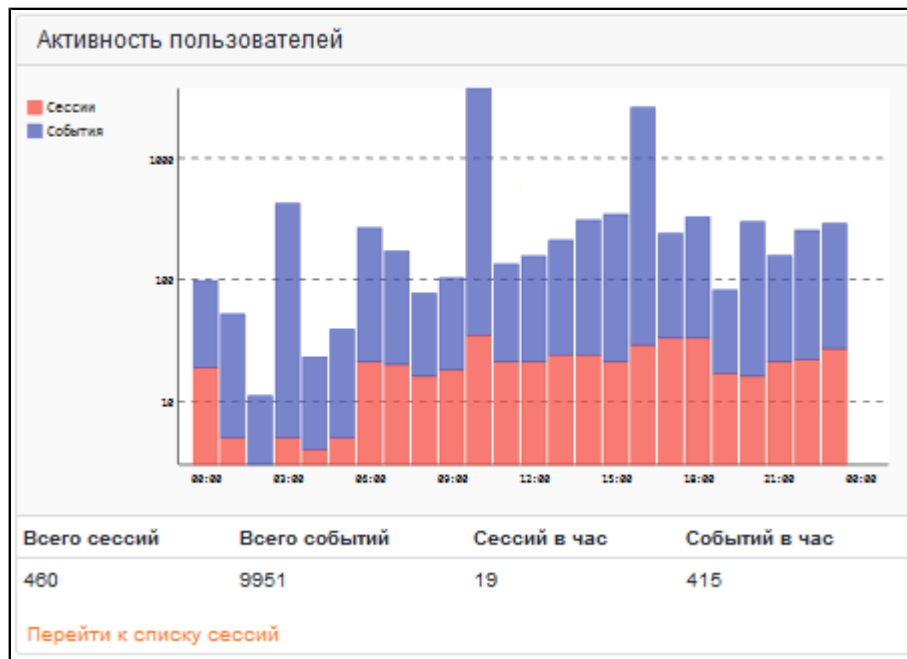


Рисунок 5 – Активность пользователей

В данной группе представлена гистограмма количества пользовательских сессий и событий, зафиксированных за выбранный временной промежуток. По оси ординат откладывается количество пользовательских сессий и событий, а по оси абсцисс – временные отметки. Также здесь представлено общее количество и частота зафиксированных сессий и событий. Отсюда пользователь СКДПУ НТ имеет возможность перейти к списку сессий, зафиксированных за выбранный временной промежуток (см. [раздел 9](#)).

6.3 Инциденты

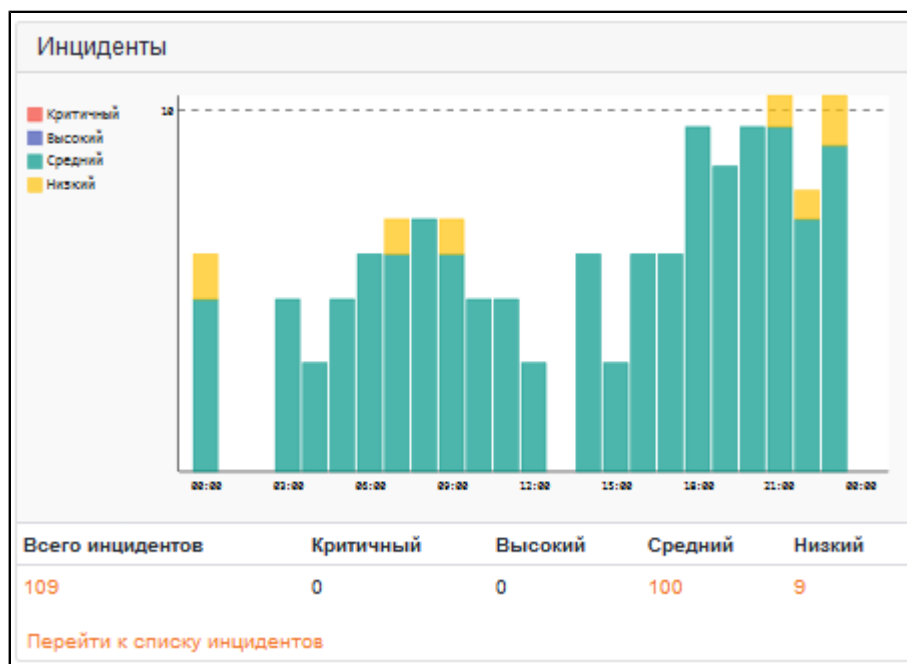


Рисунок 6 – Инциденты

В данной группе представлена гистограмма количества инициированных за выбранный временной промежуток инцидентов. Инциденты подразделяются на уровни критичности: низкий, средний, высокий, критичный. По оси ординат откладывается количество инцидентов, а по оси абсцисс – временные отметки. Также здесь представлено общее количество инцидентов и количество инцидентов каждого из уровней. Отсюда пользователь СКДПУ НТ имеет возможность перейти к подробному списку инцидентов, зафиксированных за выбранный временной промежуток.

6.4 Основные нарушители

Основные нарушители		
Персона	Уровень доверия	Инциденты
korotkovna	700	0 / 0 / 17 / 2
utkinuyu	700	0 / 0 / 14 / 0
sukharevva	700	0 / 0 / 8 / 0
senchukovai	700	0 / 0 / 5 / 0
prostyakovva	700	0 / 0 / 5 / 0

Рисунок 7 – Основные нарушители

В данной группе перечислены персоны, которые за выбранный временной промежуток инициировали наибольшее суммарное количество инцидентов. Здесь представлен их уровень

доверия и количество инициированных инцидентов, разбитых по уровням критичности в формате критичный/высокий/средний/низкий.

Пользователь СКДПУ НТ имеет возможность перейти в профили перечисленных персон (см. [раздел 8](#)).

6.5 Основные инциденты

Основные инциденты			
ID	Источник	Уровень	Статус
TF-1087480	barbolindn@passport.local	Средний	Новые
TF-1087481	senchukovai	Средний	Новые
TF-1087479	utkineyu	Средний	Новые
TF-1087478	senchukovai	Средний	Новые
TF-1087477	tabaksyurovan	Средний	Новые
Прочие инциденты...			

Рисунок 8 – Основные инциденты

В данной группе перечислены основные инциденты, которые за выбранный временной промежуток были инициированы персонами, их уровни критичности, а также текущий статус обработки. Первоначальная сортировка выполняется по уровню критичности от самого высокого до наименьшего, вторичная - по дате-времени инцидента.

Пользователь СКДПУ НТ имеет возможность перейти к полному списку инцидентов, зафиксированных за выбранный временной промежуток (см. [раздел 10.1](#)), а также перейти в профили персон, инициировавших соответствующий инцидент (см. [раздел 8](#)).

6.6 Статистика

Статистика	
Всего персон	77
Всего целевых систем	119
Всего целевых учётных записей	55
Всего загружено	628.96MB (49 файлов)
Всего скачано	3.79GB (190 файлов)
Максимум сессий в час	57

Рисунок 9 – Статистика

В данной группе представлена обобщенная статистика по количеству целевых систем и персон, чья активность была зафиксирована за выбранный временной промежуток, количеству

использованных ими учетных записей, объему загруженных и скачанных файлов (а также их количество) в течение пользовательских сессий, а также максимальное количество параллельных сессий в час.

6.7 Активные пользователи

Активные пользователи			
Персона	Сессии	Инциденты	Продолжительность
sukharevva	156	8	0:02:03
korotkovna	50	19	1 day, 23:17:33
utkineyu	25	14	1 day, 0:01:53
prostyakovva	20	5	12:30:16
solovevn	18	0	11:22:11

Рисунок 10 – Активные пользователи

В данной группе представлены самые активные персоны, активность которых была зафиксирована за выбранный временной промежуток. Также здесь представлено количество сессий каждой из перечисленных персон, количество инцидентов, инициированных каждой персоной, а также суммарная продолжительность сессий каждой из представленных персон. Персоны отсортированы в таблице по убыванию количества сессий.

Пользователь имеет возможность перейти в профиль соответствующей персоны (см. [раздел 8](#)), к списку ее сессий (см. [раздел 9](#)), рассмотреть инициированные этой персоной инциденты (см. [раздел 10.1](#)), а также перейти к списку сессий, зафиксированных за выбранный временной промежуток (см. [раздел 9.1](#)).

6.8 Активные пользователи под наблюдением

Активные пользователи под наблюдением				
Персона	Уровень доверия	Сессии	Инциденты	Продолжительность
pryazhenovaya	350	11	1	1:50:37
sokolovsa	700	3	2	2:22:30

Рисунок 11 – Активные пользователи под наблюдением

В данной группе представлены персоны, чьи действия могут нести потенциальную опасность целевым системам и обрабатываемой в них информации. Здесь приведены количество и суммарная продолжительность сессий, количество инициированных инцидентов, а также уровень доверия

каждой персоны, находящейся под наблюдением. Для попадания в данный список в карточке персоны необходимо установить отметку "Избранное".

Пользователь имеет возможность перейти в профиль соответствующей персоны (см. [раздел 8](#)), к списку ее сессий (см. [раздел 9](#)), а также рассмотреть инициированные этой персоной инциденты (см. [раздел 10.1](#)).

6.9 Активность целей

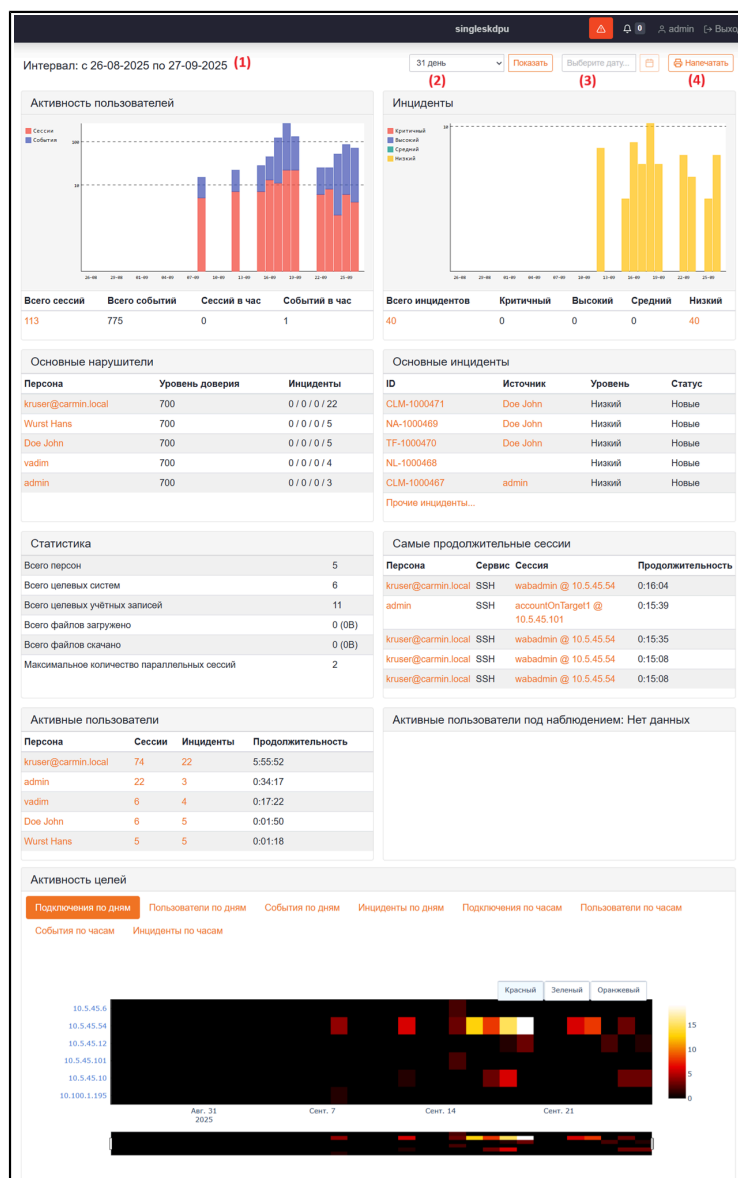


Рисунок 12 – Активность целей

Тепловая карта показывает насыщенность конкретных временных периодов по фильтрам различных отображений. Чем больше активности по выбранному фильтру в конкретный день или час, тем светлее цвет ("горячее земля").

Слева на вертикальной шкале отображаются IP-адреса целевых систем, по горизонтали временные промежутки по дням. Если выбран временной интервал больше недели, то навигация по

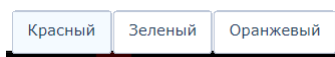
дням производится с помощью дополнительной шкалы под графиком. Передвигая нажатой левой кнопкой мыши влево или вправо, пользователь сдвигает основное отображение тепловой карты.

Также можно изменять границы отображаемых временных интервалов на тепловой карте. Для этого необходимо левой кнопкой мыши перемещать белые вертикальные столбики на вспомогательной нижней шкале отображения. Можно выбирать как более крупные интервалы дни/недели или более мелкие, такие как часы или минуты.

В верхней части меню расположены кнопки-переключатели различных отображений:

- **Подключения по дням** - отображение количества подключений к целевым системам по дням;
- **Пользователи по дням** - отображение количества подключенных пользователей к одной целевой системе по дням;
- **События по дням** - отображение количества событий на одной целевой системе по дням;
- **Инциденты по дням** - отображение количества инцидентов на одной целевой системе по дням;
- **Подключения по часам** - отображение количества подключений к целевым системам по часам;
- **Пользователи по часам** - отображение количества подключенных пользователей к одной цели по часам;
- **События по часам** - отображение количества событий на одной целевой системе по часам;
- **Инциденты по часам** - отображение количества инцидентов на одной целевой системе по часам.

Меню в правой верхней части тепловой карты нужно для выбора цветовой схемы отображения:



- Красный;
- Зеленый;
- Оранжевый.

По умолчанию стоит красная схема отображения.

Также в правом углу при наведении курсора мышки появляется меню для изменения графического отображения тепловой карты.



При наведении на иконки всплывают подсказки о выполняемых действиях.

7 ОТЧЕТЫ

7.1 Общие сведения

СКДПУ НТ в разделе веб-интерфейса **Отчеты** предоставляет функционал по генерации отчетов различных типов, а также позволяет настраивать периодичность генерации отчетов и их последующей отправки ответственным лицам по электронной почте.

Пользователь СКДПУ НТ выбирает необходимый тип отчета из перечня, представленного в разделе **Отчеты**→**Библиотека отчетов**, настраивает предварительно созданный профиль выполнения в разделе **Отчеты**→**Профили выполнения**. Все доступные для текущего пользователя СКДПУ НТ отчеты перечислены в разделе **Отчеты**→**Отчеты**. Раздел **Отчеты**→**История выполнения** содержит историю генерации настроенных текущим пользователем СКДПУ НТ отчетов.



Доступ к профилям выполнения и связанным с ними отчетам имеют только пользователи, которые их создали.

Раздел веб-интерфейса СКДПУ НТ **Отчеты** содержит следующие разделы:

- **Отчеты;**
- **Библиотека отчетов;**
- **История выполнения;**
- **Профили выполнения;**
- **Журнал авторизации.**

7.2 Отчеты

В рассматриваемом разделе перечислены отчеты, которые были настроены текущим пользователем СКДПУ НТ.

Пользователь имеет возможность сгенерировать отчет, изменить параметры настройки генерации созданных им отчетов, а также удалить выбранный отчет (см. [рисунок 13](#)).

По умолчанию, каждый пользователь имеет свой профиль выполнения и может использовать его для запуска и отправки отчетов на свой адрес email. При необходимости, пользователь может создать разные профили выполнения - с разными расписаниями, адресатами и другими параметрами и назначить требуемые отчеты на них.

Пользователь может явно указать в профиле выполнения, кто кроме него должен получить отчеты, через указание email адресатов.



Данные, составляющие отчеты, доступны пользователю в объеме и составе заданных прав доступа, с учетом Роли и действующих для роли DAR (ограничений доступа к данным). Таким образом, в отчет не попадают данные, доступ к которым пользователю запрещен.

Состав доступных шаблонов отчетов зависит от состава и параметров лицензии на подсистему.

Имя Профили выполнения	Дата последнего выполнения	Действия
Top duration sessions for 3 month 3:00	2020-04-07 19:50:03	Выполнить свймас Редактировать параметры Удалить
Sessions for 3 month 3:00	2020-05-04 19:50:04	Выполнить свймас Редактировать параметры Удалить
Persons with Incidents this monts 3:00	2020-04-07 19:50:03	Выполнить свймас Редактировать параметры Удалить
Top active persons with maximum targets for 30days 3:00	2020-05-04 19:50:04	Выполнить свймас Редактировать параметры Удалить
Persons with incidents for 3 month 3:00	2020-04-07 19:50:03	Выполнить свймас Редактировать параметры Удалить

Рисунок 13 – Раздел **Отчеты** > **Отчеты**

7.3 Библиотека отчетов

В рассматриваемом разделе перечислены доступные для создания отчеты, предварительно разбитые на следующие группы:


- **Общие отчеты по системе** содержат информацию по пользовательским сессиям выбранной целевой системы, учетным записям персон;
- **Отчеты по текущей активности** содержат информацию о целевых системах и пользовательских сессиях, зафиксированных в них в выбранный временной промежуток;
- **Отчеты по использованию** содержат сведения об использовании целевых систем, учетных записей персон, а также об активности персон;
- **Отчеты по безопасности** содержат информацию о регистрируемых в целевых системах событиях безопасности;
- **Инциденты** – это группа отчетов, которые содержат информацию об основных нарушителях безопасности на целевых системах, сведения об инцидентах с различными текущими статусами;
- **Функционирование системы** - данная группа отчетов будет добавлена позднее.

Отчет определяется через механизм (шаблон) для генерации и параметры выборки и представления данных.

В максимальном составе параметры подразделяются на следующие функциональные группы:

- 1) период времени для отбора данных (относительный "вчера" или абсолютный период времени (с-по)) - обязательные поля;
- 2) фильтры на включение (пусто = все включается, не пусто - включается только указанное);
- 3) фильтры на исключение (пусто = ничего не исключается, не пусто - указанное исключается);
- 4) настройки группировки, сортировки;
- 5) отображаемые колонки.

Не все отчеты содержат все эти параметры. Например в отчете "Обобщенная справка" модуль отчета имеет минимальный доступный состав параметров, т.к. это задано логикой отчета.

Заполненные параметры отчета можно проверить, нажав на кнопку  для формирования предварительного просмотра.

Готовые отчеты можно сохранить как именованные профили в списке личных отчетов и указать им один или несколько профилей выполнения, в соответствии с которыми подсистема будет их исполнять и доставлять указанным адресатам.

На базе одного шаблона отчетов СКДПУ НТ позволяет сохранить более одного профиля отчета, при этом параметры шаблонов отчетов позволяют в значительной мере менять представление и состав выдаваемых данных для лучшего соответствия пользовательским сценариям.

С описанием отчетов можно ознакомиться в [приложении Б](#).

7.3.1 Создание отчета

Для создания нового отчета необходимо:

Шаг 1. В разделе **Отчеты**→**Библиотека отчетов** выбрать соответствующий тип отчета, например, *Обзорный отчет по сессиям*. Подробнее о доступных типах отчетов (см. [раздел 7.3](#)).

Шаг 2. В появившейся форме заполнить необходимые поля (обязательные поля период или интервал дат)

Шаг 3. Сохранить отчет нажатием на кнопку 



Пользователь СКДПУ НТ имеет возможность предварительно посмотреть результаты генерирования отчета нажатием на кнопку [Просмотр](#). Отчет может быть просмотрен только в том случае, если выбрана дата или другой временной интервал, иначе будет выдано сообщение об ошибке. Количество записей в просмотре ограничено, по умолчанию в нем содержится 100 строк, это задается соответствующей настройкой.

Шаг 4. Указать профиль выполнения и наименование отчета. При необходимости можно указать несколько профилей.



Для создания необходимых профилей выполнения см. [раздел 7.6.1](#).

Шаг 5. Сохранить отчет нажатием на кнопку [Сохранить](#).

При успешном создании отчета появится оповещение

Отчёт сохранён успешно ×

7.3.2 Редактирование отчета

Для редактирования отчета необходимо:

Шаг 1. В разделе **Отчеты**→**Отчеты** в строке отчета нажать на кнопку [Редактировать параметры](#).

Шаг 2. В появившейся форме изменить необходимые поля.

Шаг 3. Сохранить внесенные изменения нажатием на кнопку [Сохранить](#).

При успешном сохранении отчета появится оповещение

Отчёт успешно обновлён ×

7.3.3 Удаление отчета

Для удаления отчета необходимо:

Шаг 1. В разделе **Отчеты**→**Отчеты** в строке отчета нажать на кнопку [удалить](#).

Имя Профили выполнения	Дата последнего выполнения	Действия
Test_Report 08:00	Никогда	Выполнить сейчас Редактировать параметры удалить

При успешном удалении отчета появится оповещение

Отчёт удалён успешно ×

7.3.4 Генерирование отчета

Для генерирования отчета по требованию необходимо:

Шаг 1. В разделе **Отчеты**→**Отчеты** в строке отчета нажать на кнопку Выполнить сейчас

Имя Профили выполнения	Дата последнего выполнения	Действия
Test_Report 08:00	Никогда	Выполнить сейчас Редактировать параметры Удалить

При успешном выполнении отчет добавится в историю выполнения

Отчёт: Test_Report Выполнить сейчас Редактировать отчет

Тип:	Статистика по сессиям за период
Дата создания:	2020-05-22 08:30:38
Профили:	Test
Параметры:	Группировка По целевой системе Диапазон дат этот месяц Сортировка Поле группировки По возрастаню Нет
Дата следующего выполнения:	2020-05-23 08:25:00

2020-05-22

Время выполнения: 08:31:10	Статус: Создан	Скачивание <input checked="" type="radio"/> HTML <input type="radio"/> CSV
-------------------------------	-------------------	---

Также появится оповещение

Отчёт добавлен на выполнение



Создание сложного отчета за большой период может занимать значительное время, которое может зависеть от количества записей, зарегистрированных в подсистеме и характеристик сервера СКДПУ НТ.

7.4 Кастомизация отчетов

СКДПУ НТ предоставляет возможность при создании отчета (см. [раздел 7.3.1](#)) выбрать только те сведения, которые необходимо отражать в отчетах пользователю в рамках выполнения его служебных обязанностей.

Перечень доступных к выбору сведений зависит от выбора конкретного шаблона отчета. К примеру, для **Обзорного отчета по сессиям** можно указать столбцы, которые будут выводиться в отчете: количество сессий, продолжительность сессий, сколько файлов загружено, сколько файлов скачано, какой объем данных загружен и другие. В то время как в отчете об **Ошибках авторизации** можно добавить к выводу информацию об уровне критичности, причину ошибки и другие.

Пользователь имеет возможность также указать критерии сортировки и группировки данных пользовательских сессий.

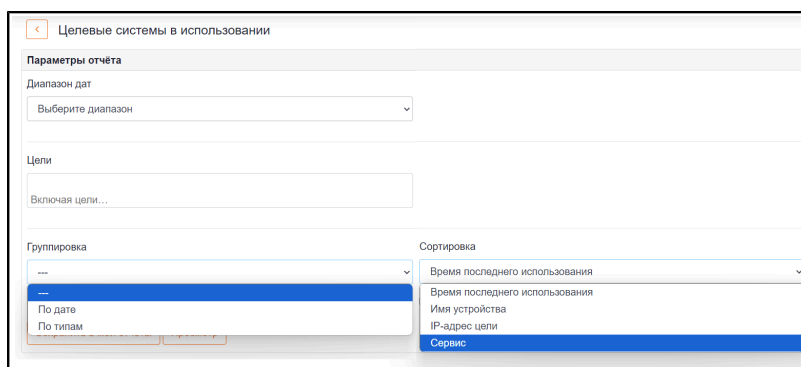


Рисунок 14 – Пример группировки и сортировки в отчете

Дополнительно некоторые отчеты позволяют установить правила обработки учетных записей: их можно исключить, включить или вывести только заданные.

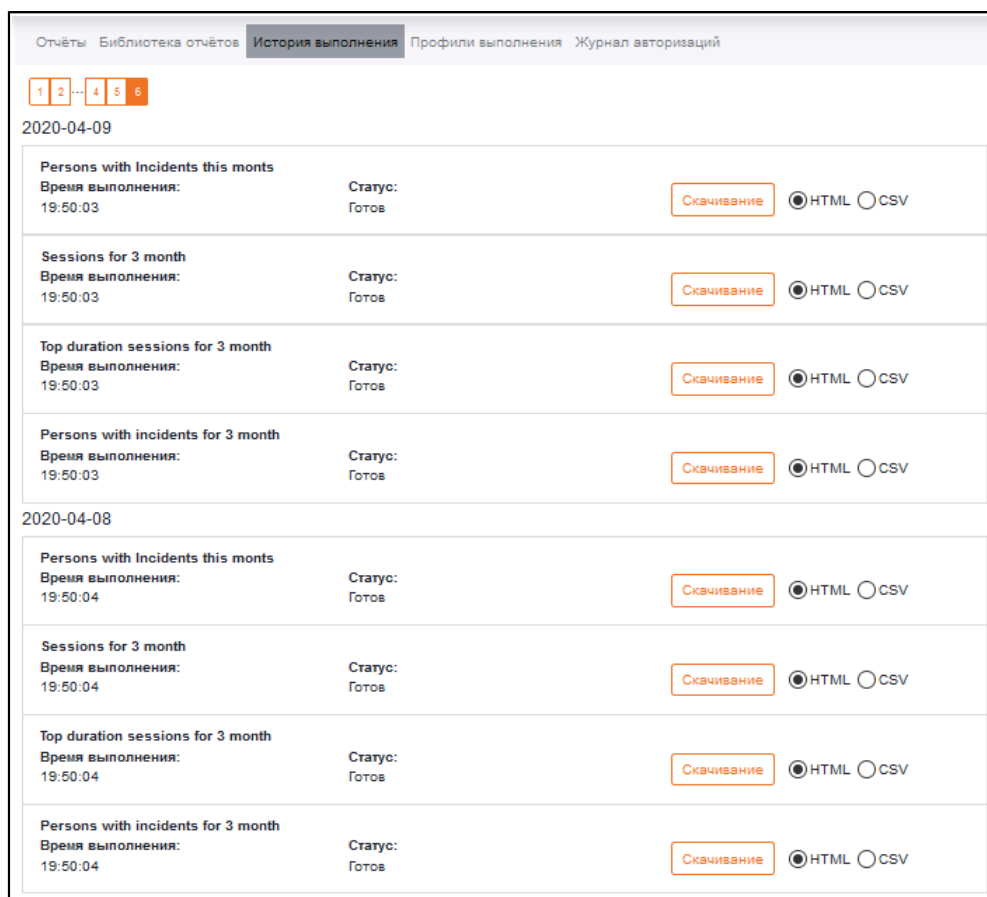
СКДПУ НТ позволяет сохранить кастомизированные отчеты для выполнения в список отчетов оператора, выполнять их далее вручную и по заданному расписанию.

7.5 История выполнения

В рассматриваемом разделе перечислены доступные для текущего пользователя СКДПУ НТ отчеты, генерация которых происходила согласно настроенному профилю выполнения (см. [раздел 7.6](#)). Также пользователь имеет возможность скачать необходимый ему отчет в соответствующем формате (см. [раздел 7.5.1](#)).

Все отчеты по умолчанию хранятся в течение трех месяцев (срок хранения отчетов может быть изменен администратором или пользователем с наличием прав на изменения настроек СКДПУ НТ). На протяжении всего срока хранения они доступны для скачивания.

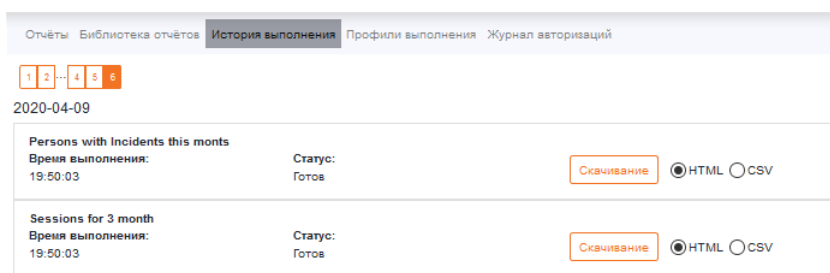
Ниже представлен фрагмент рассматриваемого раздела (см. [рисунок 15](#)).

Рисунок 15 – Раздел **Отчеты > История выполнения**

7.5.1 Скачивание отчета

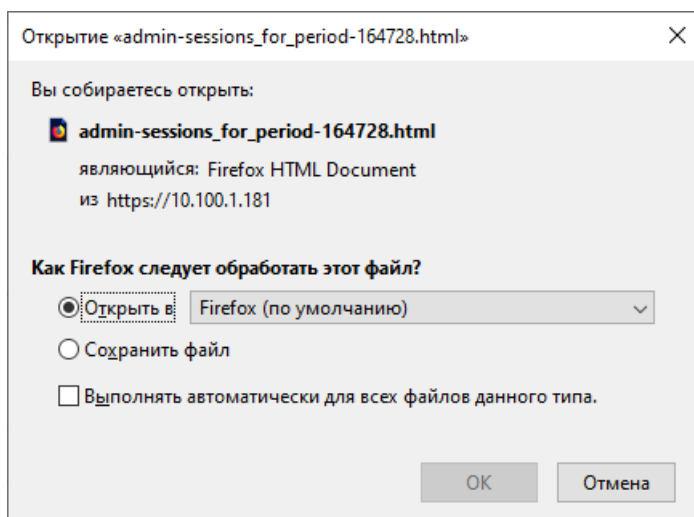
Для скачивания отчета необходимо:

Шаг 1. В разделе **Отчеты→История выполнения** в строке выбранного отчета выбрать формат отчета и нажать на кнопку **Скачивание**



Для просмотра отчета в формате CSV в Microsoft Excel, необходимо использовать инструмент *Импорт* панели инструментов **Данные**.

Шаг 2. Далее следовать указаниям диалогового окна



7.6 Профили выполнения

В рассматриваемом разделе представлен перечень профилей выполнения, которые доступны текущему пользователю СКДПУ НТ для редактирования и удаления (см. [рисунок 16](#)).

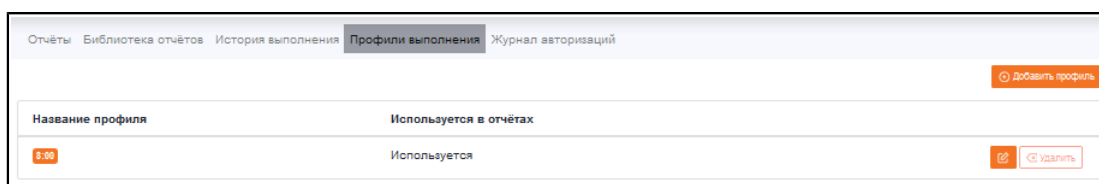


Рисунок 16 – Раздел **Отчеты > Профили выполнения**

С помощью профиля выполнения пользователь СКДПУ НТ имеет возможность настроить периодичность генерации отчета, указать адресатов, а также выбрать язык, на котором будет выполнен отчет, и формат (HTML, CSV).

Выполнение отправления ассоциированного с профилем выполнения отчета может происходить со следующей периодичностью:

- Ежедневно с указанием времени отправления.
- Еженедельно с указанием дня недели и временем отправления.
- Ежемесячно с указанием даты и времени отправления.
- Однократно с указанием даты и времени отправления.

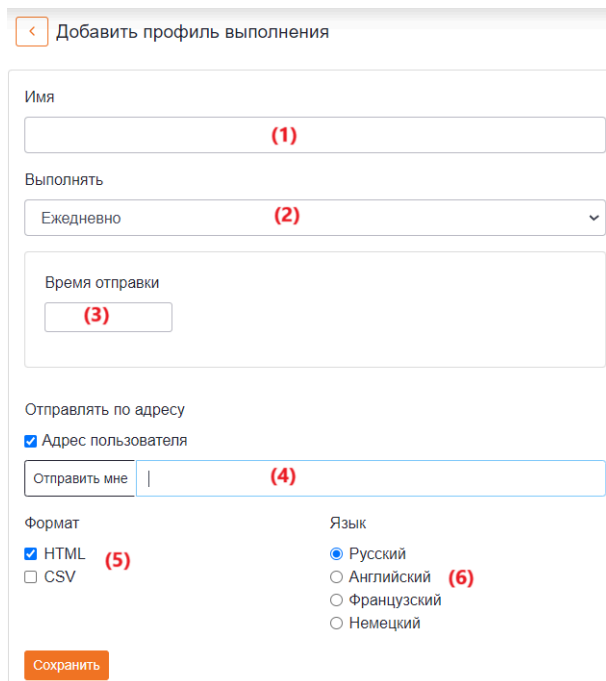
Отчеты, генерируемые согласно настройкам профиля выполнения, доступны пользователю СКДПУ НТ, который создал соответствующий профиль. Для предоставления доступа к отчетам другим пользователям необходимо указать их в списке адресатов при создании или редактировании профиля выполнения, при этом изменять настройки чужого отчета другие пользователи в подсистеме не могут.

7.6.1 Создание профиля выполнения

Для создания нового профиля выполнения необходимо:

Шаг 1. В разделе **Отчеты**→**Профиль выполнения** нажать на кнопку  .

Шаг 2. В появившейся форме заполнить необходимые поля



Добавить профиль выполнения

Имя

Выполнять

Время отправки

Отправлять по адресу

Адрес пользователя

Отправить мне |

Формат HTML (5) CSV

Язык Русский (6) Английский Французский Немецкий

(1) – идентификатор профиля;

(2) – периодичность выполнения:

- ежедневно;
- еженедельно;
- ежемесячно;
- однократно.

(3) – время отправки отчета;

(4) – электронные адреса адресатов;



Пользователь СКДПУ НТ может указывать собственный адрес, а также список других адресов получателей в рамках профиля. Электронные адреса указываются через запятую.



Пользователь СКДПУ НТ, создающий профиль запуска отчета, может добавить свой адрес электронной почты для доставки отчета (адрес, указанный в его профиле пользователя) нажатием на кнопку **Отправить мне**




. При этом его адрес будет добавлен в список адресов доставки в явном виде.

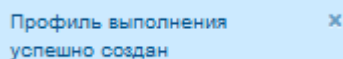
Установка флага **Адрес отправителя** инициирует получение адреса создателя профиля отчета из самого профиля каждый раз при формировании отчета. В этом случае отчет будет отправлен на актуальный адрес, указанный в профиле пользователя на момент отправки отчета, в отличие от первого варианта, когда адрес сохранен в явном виде и не обновляется после изменения адреса в профиле пользователя.

Электронные адреса указываются через запятую.

- (5) – формат генерируемого отчета;
- (6) – язык представления данных в отчете.


Шаг 3. Сохранить профиль нажатием на кнопку  .

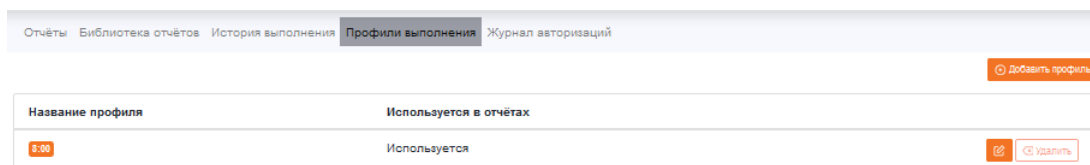
При успешном создании профиля выполнения появится оповещение







7.6.2 Редактирование профиля выполнения

Для редактирования профиля выполнения необходимо:

Шаг 1. В разделе **Отчеты**→**Профиль выполнения** в строке редактируемого профиля выполнения нажать на кнопку 



Отчеты Библиотека отчетов История выполнения Профили выполнения Журнал авторизаций	
	
Название профиля	Используется в отчетах
	Используется  

Шаг 2. В появившейся форме изменить желаемые настройки

Имя
19:30

Выполнять
Ежедневно

Время отправки
19:30

Отправлять по адресу
Отправить мне `mailto:prof@vashsite.ru`

Формат
 HTML
 CSV

Язык
 Русский
 Английский
 Французский
 Немецкий

Сохранить

Шаг 3. Зафиксировать изменения нажатием на кнопку **Сохранить**.

При успешном сохранении изменений параметров профиля выполнения появится оповещение

Профиль выполнения успешно обновлён

7.6.3 Удаление профиля выполнения

Для удаления профиля выполнения необходимо:

Шаг 1. В разделе **Отчеты**→**Профиль выполнения** в строке профиля выполнения, который следует удалить, нажать на кнопку **Удалить**.

Отчеты		Библиотека отчетов		История выполнения		Профили выполнения		Журнал авторизаций	
Добавить профиль									
Название профиля			Используется в отчетах						
5:30			Используется		Удалить				

Шаг 2. Подтвердить удаление в диалоговом окне.



Профиль выполнения, ассоциированный хотя бы с одним отчетом, удалить нельзя. Необходимо удостовериться, что профиль выполнения не используется ни в одном отчете.

При успешном удалении профиля выполнения появится оповещение

Профиль выполнения удалён

8 ПЕРСОНЫ

8.1 Общие сведения

В разделе веб-интерфейса **Персоны** СКДПУ НТ представлен перечень идентификаторов персон. Карточки персон формируются подсистемой автоматически на основании анализа событий сессий. Администраторы подсистемы могут дополнительно вносить свои исправления и пометки в профиль персоны вручную. Карточка персоны отражает накопленные подсистемой сведения об активности определенного пользователя в рамках сессий удаленного доступа.

У одного человека может быть более одной учетной записи, с помощью которых он пользуется удаленным доступом. Подсистема позволяет учесть такие ситуации, сохраняя для карточки персоны все идентификаторы учетных записей по пользователю.

С каждой персоной связан индивидуальный количественный показатель – Уровень доверия (см. [раздел 8.2](#)), который рассчитывается с учетом уровня критичности инициированных этой персоной инцидентов и их количеством (см. [рисунок 17](#)).

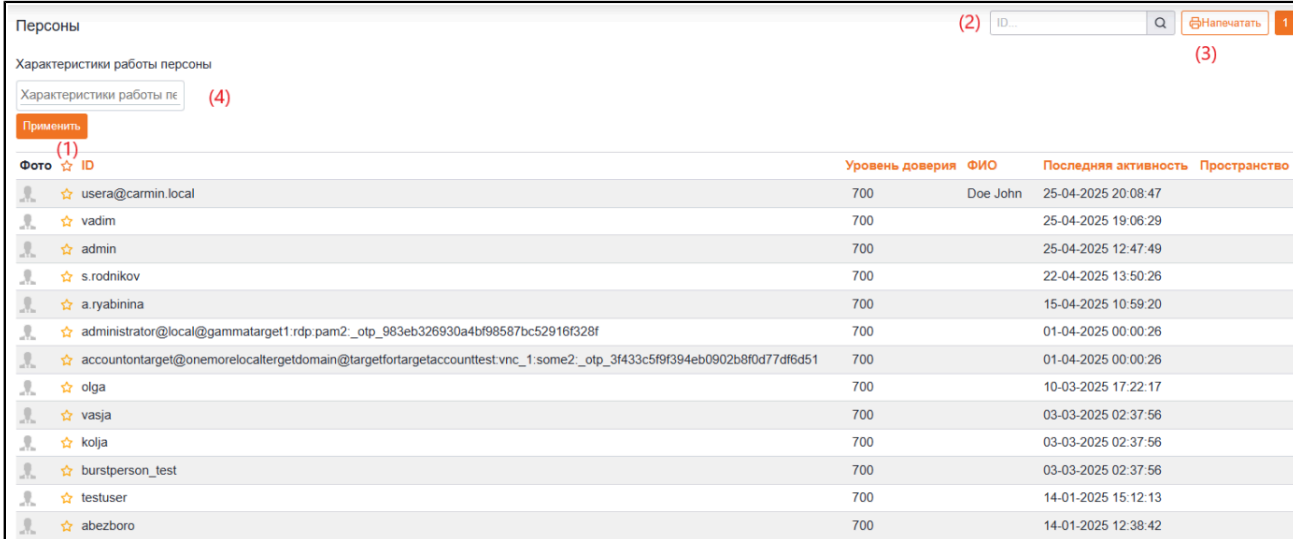



Фото	ID	Уровень доверия	ФИО	Последняя активность	Пространство
☆	usera@carmin.local	700	Doe John	25-04-2025 20:08:47	
☆	vadim	700		25-04-2025 19:06:29	
☆	admin	700		25-04-2025 12:47:49	
☆	s.rodnikov	700		22-04-2025 13:50:26	
☆	a.ryabinina	700		15-04-2025 10:59:20	
☆	administrator@local@gammatarget1.rdp.pam2_otp_983eb326930a4bf98587bc52916f328f	700		01-04-2025 00:00:26	
☆	accountntarget@onemorelocaltargetdomain@targetfortargetaccounttest.vnc_1:some2_otp_3f433c5f9f394eb0902b8f0d77df6d51	700		01-04-2025 00:00:26	
☆	olga	700		10-03-2025 17:22:17	
☆	vasja	700		03-03-2025 02:37:56	
☆	kolja	700		03-03-2025 02:37:56	
☆	burstperson_test	700		03-03-2025 02:37:56	
☆	testuser	700		14-01-2025 15:12:13	
☆	abezboro	700		14-01-2025 12:38:42	

Рисунок 17 – Раздел **Персоны**

Уровень доверия рассчитывается подсистемой автоматически и учитывается при анализе поступающих данных и реакциях подсистемы на них. Администратор безопасности при необходимости может вносить правки в значения уровня доверия. Пользователи без прав доступа к профилям персон изменять уровень доверия не могут. При отсутствии инцидентов значение показателя постепенно восстанавливается до нормального.

Из перечня персон можно выбрать тех, которых следует взять под наблюдение, активировав элемент (1).

После анализа данных сессий персоны могут быть промаркированы и сгруппированы по каким-то общим признакам (тегам) на основе накопленных данных о персоне. СКДПУ НТ дает возможность отфильтровать персоны со схожим поведением или характеристиками, основываясь

на тегах персон. Для этого необходимо выбрать нужные характеристики из выпадающего списка в поле **Характеристики работы персоны** (4) и нажать на кнопку **Применить** . Можно выбрать несколько характеристик. Подсистема отфильтрует пользователей по заданным характеристикам (с логикой AND).

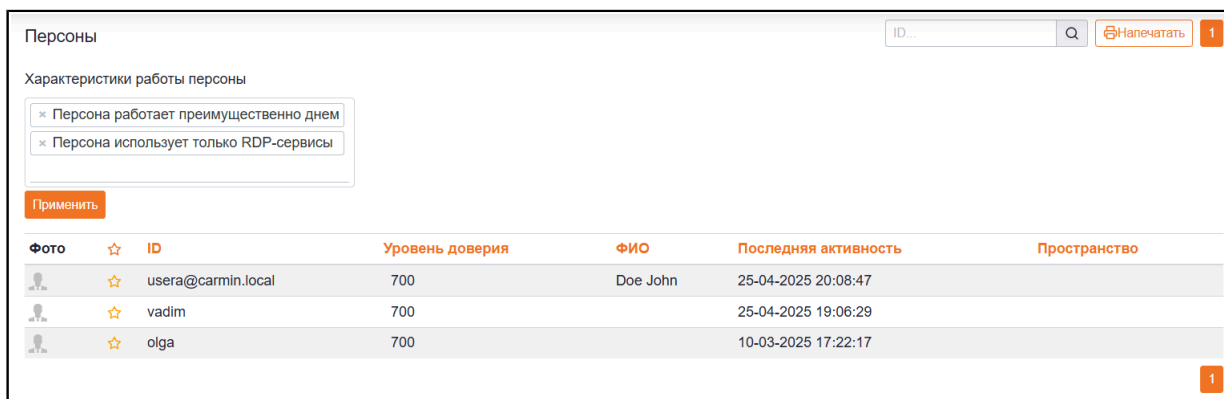


Рисунок 18 – Фильтр пользователей по тегам

С каждой персоной в СКДПУ НТ связан цифровой профиль персоны (см. [раздел 8.5](#)). Для доступа к цифровому профилю персоны необходимо выбрать интересующую персону из перечня в разделе **Персоны**.

Также имеется возможность найти персону, введя ее идентификатор в строку поиска (2).

Данные о персонах могут быть распечатаны с использованием кнопки **Напечатать**  (3).

8.2 Уровень доверия

За каждой персоной закреплен количественный показатель «Уровень доверия», который представляет собой численное отражение оценки риска по данной персоне по результатам анализа, формирующийся с учетом накопленной статистики ее аномального поведения.

При генерации инцидента, источником которого является персона, значение уровня доверия уменьшается на величину, равную влиянию инцидента, который рассчитывается с учетом весового коэффициента инцидента.

Накопленные изменения уровня доверия фиксируются в цифровом профиле персоны в виде истории значений. При отсутствии инцидентов за некоторый период времени значение уровня доверия постепенно восстанавливается в первоначально заданное значение (по умолчанию 700 единиц).



Рисунок 19 – Цифровой профиль пользователя - уровень доверия

На графике выводится последние 50 значений уровня доверия, каждые сутки значение уровня доверия восстанавливается на 50 единиц.

8.3 Склеивание персон

В СКДПУ НТ реализован механизм принудительного (ручного) агрегирования нескольких персон под одним идентификатором для возможности использовать данные, накопленные по всем персонам, совместно (для просмотра и анализа). Это необходимо тогда, когда пользователь шлюзов в контуре использует разные логины для входа на шлюз, но на самом деле является одной и той же персоной. "Склеивание" персон позволяет офицеру безопасности в полном объеме анализировать данные по персоне.

В результате операции "склеивания" в подсистеме будет создан такой профиль персоны, который включает идентификаторы всех склеенных персон. Сессии по этим идентификаторам будут обрабатываться как принадлежащие данному профилю персоны. Остальные профили персон, которые были приклеены, подсистема забывает (см. [раздел 8.4](#)).

Все "склеенные" логины будут отображаться в карточке персоны (см. [раздел 8.5](#)). В таблице персон на вкладке **Персоны** будет отображаться основной аккаунт (первый, к которому были совершены склейки).

Процедура склеивания персон доступна только Администратору подсистемы с определенными правами доступа.



Склеенные персоны принадлежат одному пространству.

8.4 Забывание персон

В подсистеме в рамках требований 152-ФЗ "О персональных данных" и Общего регламента по защите персональных данных Евросоюза (GDPR) реализована возможность произвести по требованию "забвение" данных, накопленных о какой-либо персоне до текущего момента, без потери целостности хранимых данных.

Механизм "забывания" персоны используется также в случае, когда необходимо начать накопление данных по персоне заново, не дожидаясь срока истечения ретенции. Для этого в существующей записи о персоне изменяется логин первичной авторизации на шлюзе, по которому осуществлялась ранее группировка событий сессии персоны. В результате данные о прошлых сессиях в подсистеме сохраняются, а карточка персоны с таким логином будет создана заново в момент совершения ей новой сессии. И далее все накопление статистики начнется снова.

Персона также считается забытой, если она была "приклеена" к другой персоне. При этом накопленные до момента склейки данные перемещены в основную персону не будут.

Забывтые персоны могут быть просмотрены в разделе **Персоны** до момента автоматической очистки архива (выхода срока ретенции). Они идентифицируются в таблице по префиксу *forgotten@*.

Процедура забывания персон доступна только Администратору подсистемы с определенными правами доступа.



Персона (пользователь шлюза) с *forgotten@* в аккаунте, не относящаяся к забытым персонам, будет обрабатываться по правилам обработки забытых персон.

8.5 Цифровой профиль персоны

Цифровой профиль персоны содержит общую информацию о персоне (1), графическое представление истории изменений **Уровня доверия** (2), данные об активности персоны в целевых системах (3), а также статистику по инициированным за все время инцидентам (4) (см. [рисунок 20](#)).

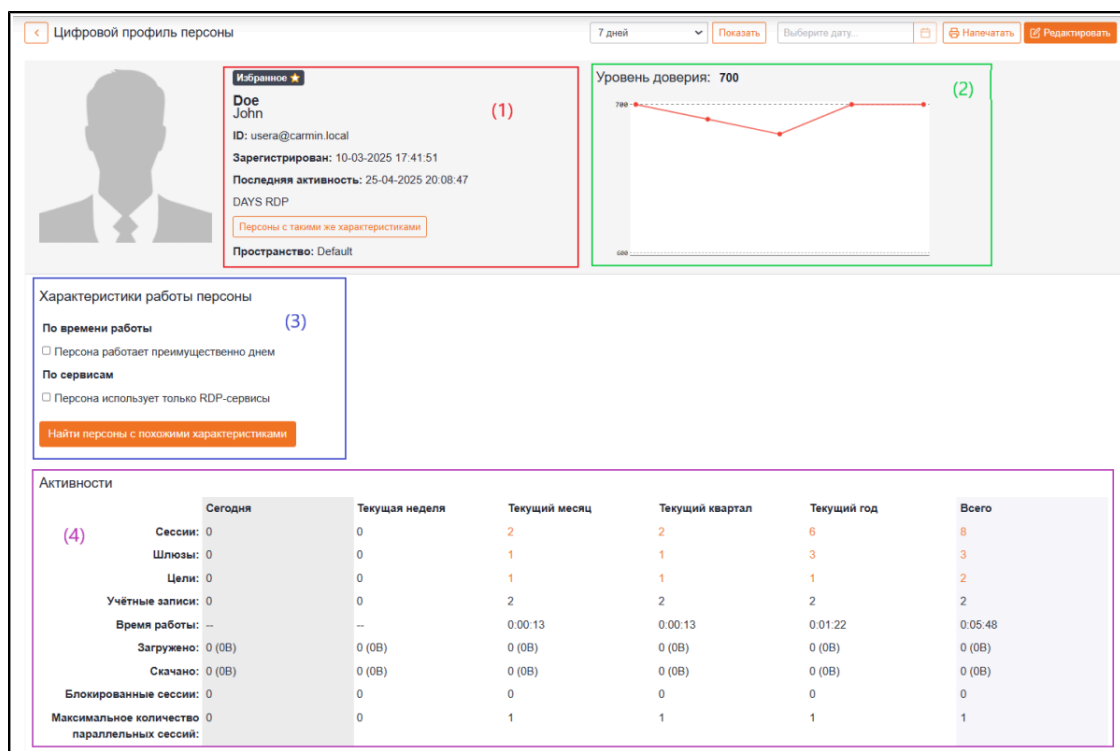


Рисунок 20 – Цифровой профиль пользователя

Для персон, к которым приклеивали данные (см. раздел 8.3), в идентификаторе будут отображаться все идентификаторы приклеенных персон. Первый логин считается основным, тем, к которому было приклеивание. Из остальных использованных в операции карточек персон удаляется вся адресная информация через процедуру забвения персоны (см. раздел 8.4). В таком идентификаторе будет стоять логин *forgotten@uuid*.

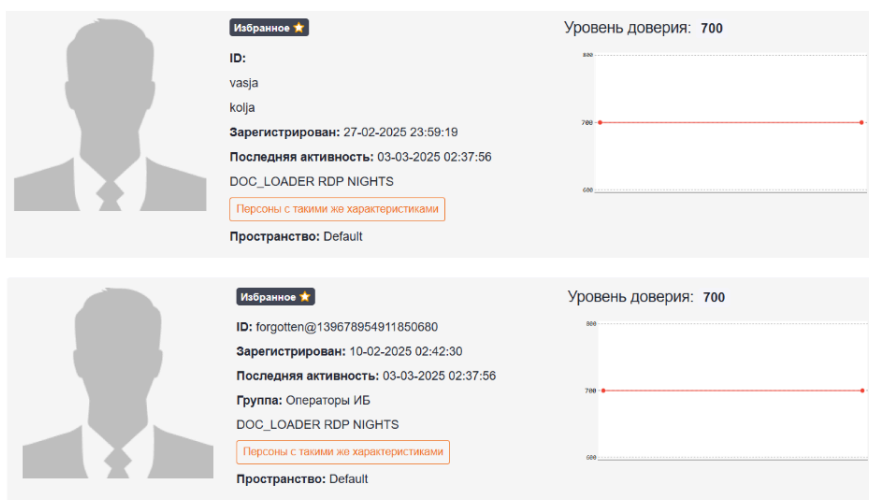


Рисунок 21 – Управление персонами (склеивание и забывание)


В цифровом профиле персоны также представлена оперативная статистика по ее сессиям, инцидентам за выбранный временной промежуток.


В СКДПУ НТ имеется возможность получить статистические данные за определенный временной промежуток в соответствии с выбранными значениями.

Для выбора доступны следующие временные промежутки:



- за текущий день;
- за предыдущий день;
- за последние семь дней;
- за последний тридцать один день.

Подтверждение осуществляется нажатием на кнопку .


Также пользователь имеет возможность выбрать для просмотра конкретную дату, подтвердив нажатием на кнопку .

Пользователь может оперативно напечатать сводную статистику за выбранный ранее временной промежуток, нажав на кнопку .

При наличии прав на просмотр пользователь СКДПУ НТ имеет возможность перейти в соответствующие разделы для более подробного анализа данных, выбрав активные ссылки, выделенные цветом.

Пользователь может найти персоны с такими же характеристиками, как у данной персоны. Для этого необходимо нажать на кнопку **Персоны с такими же характеристиками**  в поле общей информации о персоне (1) или выбрать нужные характеристики в поле **Характеристики работы персоны** (3) и нажать на кнопку **Найти персоны с похожими характеристиками** . Подсистема вернет пользователя в общий раздел **Персоны** и отфильтрует таблицу с персонами в соответствии с выбранными характеристиками.



При нажатии кнопки **Персоны с такими же характеристиками**  персоны будут отфильтрованы по всем тегам, которыми маркирована данная персона, с логикой AND.

8.5.1 Редактирование информации о персоне

Для редактирования информации о персоне для конкретизации функциональных обязанностей в целях повышения эффективности проведения расследования инициированных ими инцидентов информационной безопасности необходимо:



Редактирование возможно только при наличии соответствующих прав. Персону с префиксом *forgotten@* отредактировать нельзя.

Шаг 1. В разделе веб-интерфейса **Персоны** выбрать персону из списка нажатием левой кнопки мыши

Персоны

Характеристики работы персоны

Характеристики работы пе

Применять

Фото	ID	Уровень доверия	ФИО	Последняя активность	Пространство
	admin	700		16-06-2025 15:42:33	
	s.rodnikov	700		16-06-2025 14:14:47	
	uservasya	700		01-06-2025 00:00:28	
	vadim	700		22-05-2025 12:18:21	
	olga@carmin.local	700		19-05-2025 15:35:15	realm 1
	usera@carmin.local	700	Doe John	13-05-2025 14:57:35	
	a.gyabinina	700		15-04-2025 10:59:20	



Цифровой профиль персоны

7 дней Показать Выберите дату

Напечатать Редактировать

Ибранное *

ID: s.rodnikov

Зарегистрирован: 10-04-2025 12:18:44

Последняя активность: 16-06-2025 14:14:47

SSH DAYS

Персоны с такими же характеристиками

Пространство: Default

Уровень доверия: 700

В цифровом профиле персоны отображается идентификатор персоны, дата регистрации персоны в целевой системе, дата последнего подключения к целевой системе, а также данные, которые указываются на [Шаг 3](#)

Шаг 2. Нажать на кнопку Редактировать

Шаг 3. В появившейся форме внести изменения в данные персоны

Цифровой профиль пользователя

Фото

(1)

Фамилия

(2)

Имя

(3)

Отчество

(4)

Подразделение

(5)

Должность

(6)

Группа

Интеграторы (7)

Сохранить

Для персоны предоставляется возможность указать следующие данные:

- (1) - фотография персоны;




Для использования в качестве изображений персон поддерживаются форматы файлов jpeg, jpg, png, размером не более 1 мб.

- (2) - фамилия;
- (3) - имя;
- (4) - отчество (при наличии);
- (5) - подразделение, в котором числится рассматриваемая персона;

- (6) - занимаемая должность;
- (7) - группа, к которой принадлежит персона.



Информация о персоне (ФИО, подразделение, должность) может содержаться в структуре LDAP сервера при наличии последнего.

Шаг 4. Для сохранения внесенных изменений необходимо нажать на кнопку .

При успешном сохранении параметров профиля персоны появится оповещение

Данные персоны обновлены 

9 СЕССИИ

9.1 Общие сведения

СКДПУ НТ в разделе веб-интерфейса **Сессии** предоставляет функционал для просмотра, поиска, фильтрации и сортировки пользовательских сессий целевых систем при условии наличия соответствующих прав доступа.



СКДПУ НТ имеет возможность ограничить доступ для своих пользователей к данным пользовательских сессий целевых систем с помощью списков ограничения доступа к данным (подробнее см. Руководство администратора).

Пользователь СКДПУ НТ имеет возможность осуществлять полнотекстовый анализ пользовательских сессий (1). Анализу могут быть подвергнуты:

- Текст, вводимый с клавиатуры;
- Заголовки окон, открывавшиеся в рамках сессии;
- Имена файлов;
- Имена процессов, старт которых регистрировался в рамках сессии;
- Тексты, передававшиеся через буфер обмена в рамках сессии.

На [рисунке 22](#) продемонстрирована форма для настройки поиска по пользовательским сессиям.

Рисунок 22 – Страница Сессии

Фильтрация результатов поиска происходит посредством включения (2) или исключения (3) диапазона дат, идентификатора целевого устройства (цели), адреса клиента, учетной записи (аккаунта) персоны, а также идентификатора персоны.

Группировка результатов (4) может осуществляться по дате, идентификатору целевого устройства (цели), учетной записи (аккаунта), адресу клиента или идентификатору персоны.

Результат поиска представляет собой список сессий с возможностью сортировки по количеству вхождений поисковой строки и подсветкой совпадений при просмотре.



При работе в распределенном контуре информация о новых сессиях и их метаданных узлы передают на головную машину в сообщениях довольно оперативно (порядок – минуты, десятки минут при наличии стабильной связи между узлом и головной машиной) при обработке, а головная машина при необходимости может получать от узлов актуальные списки сессий с метаданными, чтобы поддерживать у себя актуальный общий список сессий. На головную машину также передаются вторичные сущности, полученные при обработке сессий: персоны, целевые устройства, шлюзы, клиентские адреса. На головную машину не передаются списки событий в сессиях, полнотекстовые индексы. Эти данные хранятся на тех узлах, куда они пришли и были обработаны.


Фрагмент результата поиска данных пользовательских сессий целевых систем без применения фильтров продемонстрирован на [рисунке 23](#).


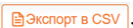
(1) Сервис	(2) Старт	(3) Продолжительность	(4) Персона / Аккаунт	(5) Адрес клиента	(6) Адрес цели	(7) Шлюз	(8) События	(9) Упаковано
SSH	22-07-2025 14:24:13	0:01:24	Vasiliy / alphatargetuser	172.16.137.14	10.5.45.10	farm- slave1	2	<input checked="" type="checkbox"/>
SSH	22-07-2025 14:21:14	0:03:23	Vasiliy / alphatargetuser	172.16.137.14	10.5.45.10	farm- slave1	2	<input checked="" type="checkbox"/>
RDP	22-07-2025 14:15:30	0:00:16	Vasiliy / Administrator	172.16.137.14	10.5.45.13	farm- slave0	38	<input checked="" type="checkbox"/>
RDP	22-07-2025 14:13:49	0:03:11	IamVas / Administrator	172.16.137.14	10.5.45.13	farm- slave0	52	<input checked="" type="checkbox"/>

Рисунок 23 – Пример выборки сессий

СКДПУ НТ по результатам поиска предоставляет информацию о пользовательских сессиях целевых систем, включающую следующие данные:

- (1) – тип сервиса
- (2) – начало пользовательской сессии подключения
- (3) – продолжительность пользовательской сессии
- (4) – идентификатор персоны и используемый аккаунт на целевой системе
- (5) – IP-адреса персоны
- (6) – IP-адрес целевого устройства
- (7) – наименование шлюза доступа, через который производилось подключение
- (8) – количество событий, зафиксированных в течение сессии
- (9) – флаг успешно закачанной в Архив аудита сессии при наличии данного функционала

При нажатии на кнопку  появляется дополнительное поле, в котором можно выбрать тип (1)-(8), где будет задана дополнительная маска для более удобного поиска.

Пользователь СКДПУ НТ может распечатать список сессий, нажав на кнопку  или сохранить данные в формате CSV, нажав на кнопку .

9.2 Профиль пользовательской сессии

Профиль пользовательской сессии содержит подробный перечень данных о выбранной сессии, необходимый для анализа активности интересующей персоны.

Для перехода к профилю пользовательской сессии необходимо из перечня пользовательских сессий (см. [рисунок 23](#)) выбрать интересующую сессию.

Кнопки **Скачать запись**, **Скачать список файлов**, **Скачать лог**, **Скачать список событий** позволяют сохранить необходимые данные по интересующей сессии. Если в сессии отсутствуют какие-то файлы, то соответствующая кнопка для скачивания не активна.

Пример профиля пользовательской сессии представлен на [рисунке 24](#). В профиле представлена общая информация о пользовательской сессии (1), а также подробный перечень действий, которые осуществлялись персоной в течение всего времени сессии (2). Каждое действие характеризуется датой и временем, типом события, а также данными, которые вводила персона во время совершения рассматриваемого действия.



В некоторых случаях пользователь СКДПУ НТ при наличии соответствующих прав доступа может просмотреть видеозапись пользовательской сессии.

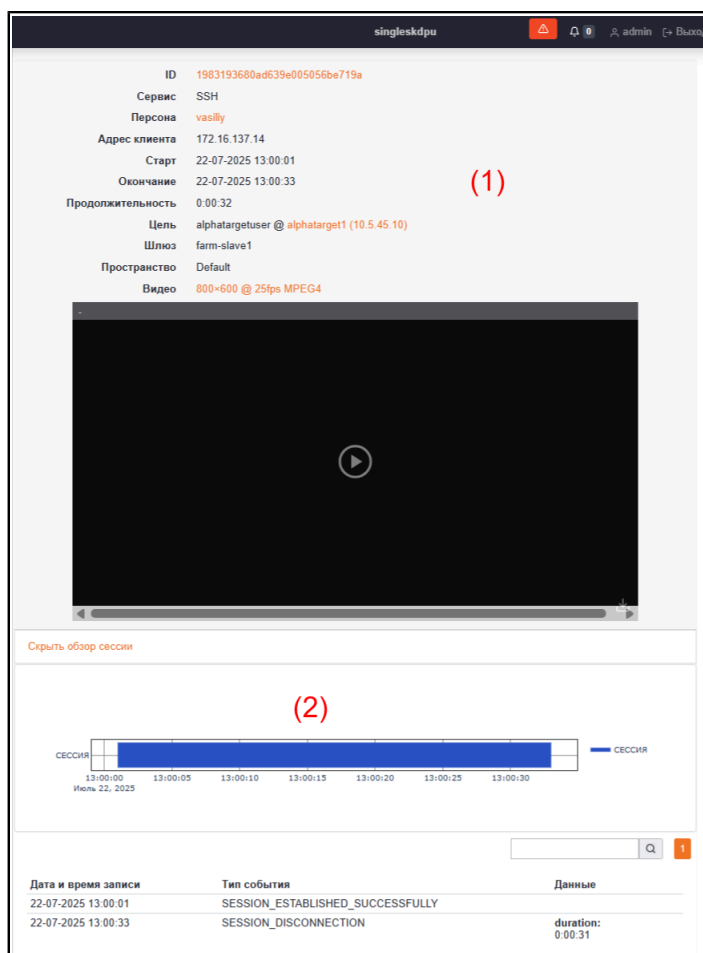



Рисунок 24 – Карточка пользовательской сессии

В карточке сессии отражены такие свойства сессии как:

- ID
- Тип сервиса
- Персона (содержит ссылку на карточку персоны)
- Клиентский адрес (содержит ссылку на карточку клиентского адреса)
- Время начала работы
- Время окончания работы
- Продолжительность
- Целевое устройство (содержит ссылку на карточку целевого устройства)
- Шлюз
- Пространство
- Плеер Аудит Архива содержит запись сессии. Плеер доступен только для завершенных сессий.

Блок **Обзор сессии** содержит диаграмму Ганта. На диаграмме по одной оси отображаются события сессии, по другой оси - время события. При наведении на элемент диаграммы появляется всплывающая подсказка с указанием названия события, даты, диапазона дат и точного времени.

Поле **Поиск** позволяет искать поисковое слово внутри списка событий сессии.

Пользователь может распечатать профиль сессии, нажав на кнопку  [Напечатать](#).

Пользователь СКДПУ НТ имеет возможность, при наличии достаточных оснований, создать инцидент непосредственно из карточки сессии, подробнее (см. [раздел 10.3](#)).

10 ИНЦИДЕНТЫ

10.1 Общие сведения

СКДПУ НТ позволяет пользователям осуществлять управление инцидентами (событиями в рамках сессий, которые потенциально могут нести угрозу информационной безопасности инфраструктуры), которые фиксируются в целевых системах с помощью детекторов аномального поведения, поведение которых заранее настраивается (см. Руководство администратора). Пользователи СКДПУ НТ могут вручную создавать инциденты (см. [раздел 10.3](#)).

Расследование инцидентов начинается с назначения ответственного лица (см. [раздел 10.5](#)), которое впоследствии обрабатывает инцидент. Обработка инцидента подразумевает под собой ряд действий со стороны ответственного лица, например, корректирование уровня критичности инцидента в рамках оценки последствий для инфраструктуры, изменение статуса инцидента и т.д. (см. [раздел 10.4](#)).

По результатам расследования инцидента происходит его закрытие с указанием причины возникновения (см. [раздел 10.6](#)).

Действия некоторых персон могут инициировать инциденты, которые таковыми не являются. СКДПУ НТ предоставляет возможность указать правила, по которым некоторые срабатывания детекторов аномалий будут игнорироваться для указанных клиентских адресов, персон или целевых устройств (см. [раздел 10.7](#)).

Все действия в течение всего времени обработки инцидента фиксируются в истории инцидента (см. [раздел 10.2](#)).

СКДПУ НТ в разделе веб-интерфейса **Инциденты** предоставляет функционал для просмотра, поиска и фильтрации инцидентов при условии наличия соответствующих прав доступа.



СКДПУ НТ имеет возможность ограничить доступ пользователей к инцидентам тех или иных персон или на тех или иных шлюзах, целевых устройствах с помощью списков ограничения доступа к данным (подробнее см. Руководство администратора).

Пользователь СКДПУ НТ имеет возможность осуществлять инцидента про ID или с использованием фильтров, предварительно настроив следующие фильтры (см. [рисунок 25](#)):

- (2) – тип инцидента;
- (3) – идентификатор персоны;
- (5) – адрес шлюза доступа;
- (6) – ответственный за обработку инцидента;
- (7) – диапазон дат, в пределах которого были зафиксированы инциденты;
- (8) – текущий статус инцидента;
- (9) – возможная причина появления инцидента;
- (10) – уровень критичности инцидента;

The screenshot shows a search interface for incidents. At the top, there is a search bar for the incident ID (1) with a 'Поиск' button. Below this are several filter sections:

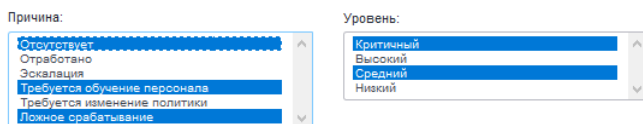
- Тип инцидента:** A dropdown menu with 'Любой' selected (2).
- Статус:** A list of status options: 'Новые', 'В работе', 'Закрытые (отработанные)', and 'Закрытые (эскалация)' (8).
- Персона:** A dropdown menu with 'Персона...' selected (3).
- Причина:** A list of cause options: 'Отсутствует', 'Отработано', 'Эскалация', 'Требуется обучение персонала', 'Требуется изменение политики', and 'Ложное срабатывание' (9).
- Адрес клиента:** A dropdown menu with 'Адрес клиента...' selected (4).
- Шлюз:** A dropdown menu with 'Шлюз...' selected (5).
- Назначен:** A dropdown menu with 'Любой' selected (6).
- Уровень:** A list of severity levels: 'Критичный', 'Высокий', 'Средний', and 'Низкий' (10).
- Период:** A field for date range selection (7).

At the bottom, there is a 'Поиск' button, a 'записей на странице' dropdown set to '25', and an 'Очистить' button.

Рисунок 25 – Раздел **Инциденты**



При фильтрации статуса, причины или уровня инцидента имеется возможность выбрать несколько значений для каждого из перечисленных фильтров, для этого необходимо нажать Ctrl и левой кнопкой мыши указать желаемые значения



Ниже представлен фрагмент результата поиска инцидентов без применения фильтров (см. [рисунок 26](#)).

Инциденты: 1443, 31-03-2023 Напечатать 1 2 3 4 5 ... 57 58 >

Добавить фильтры ▾

Параметры запроса

(1) ID	(2) Дата регистрации	(3) Источник	(4) Адрес клиента	(5) Тип инцидента	(6) Уровень	(7) Влияние	(8) Статус	(9) Причина	(10) Назначен	(11) Уведомления
AL-1001344	30-03-2023 19:30:12	downloader	100.100.100.100	Индикаторы взрывной активности	Низкий	10	Новые			
AL-1001341	30-03-2023 19:30:11	uploader	100.100.100.100	Индикаторы взрывной активности	Низкий	10	Новые			
RJ-1000202	30-03-2023 18:36:37	mycyksv	172.18.24.99	Туннели и прыжки	Высокий	30	Новые			
CLM-1001414	30-03-2023 18:34:27	volkovds	172.18.17.56	Подозрительные команды	Низкий	20	Новые			
RJ-1001071	30-03-2023 18:10:50	zharovma@passp...	172.18.17.104	Туннели и прыжки	Низкий	10	Новые			
RJ-1001411	30-03-2023 18:08:29	kurdyukovis	172.18.16.51	Туннели и прыжки	Низкий	10	Новые			
CLM-1001201	30-03-2023 18:05:19	borovikovas	172.18.17.155	Подозрительные команды	Низкий	20	Новые			
RJ-1000205	30-03-2023 18:04:27	andryuschenkoda	172.18.17.116	Туннели и прыжки	Низкий	10	Новые			

Рисунок 26 – Пример представления результатов выборки всех инцидентов

СКДПУ НТ по результатам поиска предоставляет информацию об инцидентах, включающую следующие данные:

- (1) – идентификатор инцидента.
- (2) – дата и время регистрации инцидента.
- (3) – источник инцидента.
- (4) – адрес клиента.
- (5) – тип инцидента.
- (6) – уровень критичности инцидента.
- (7) – коэффициент влияния.
- (8) – текущий статус инцидента.
- (9) – причина возникновения инцидента.
- (10) – назначенный ответственный за обработку инцидента.
- (11) – уведомления по инциденту.

При нажатии на кнопку Добавить фильтры ▾ появляется дополнительное поле, в котором можно выбрать тип (1)-(11), где будет задана дополнительная маска для более удобного поиска.

Пользователь может распечатать список инцидентов, нажав на кнопку Напечатать.

10.2 Карточка инцидента

Карточкой инцидента содержит подробный перечень данных о выбранном инциденте. Для перехода к карточке инцидента необходимо из перечня инцидентов (см. [рисунок 26](#)) выбрать интересующий инцидент.

Пример карточки инцидента представлен на [рисунке 27](#). В карточке представлена общая информация об инциденте (1), подробный перечень действий, которые инициировали инцидент (2). Каждое действие характеризуется датой и временем, типом события, а также данными, которые были введены персоной во время совершения рассматриваемого события.

i При возникновении инцидентов некоторых типов причины их возникновения отображаются в поле **Данные** области (1).

Здесь же представлена история внесения изменений в параметры инцидента (3), где отображается информация о дате и времени изменений, о том, кем были произведены изменения, и какие изменения были внесены.

Из карточки инцидента пользователь СКДПУ НТ имеет возможность просмотреть цифровой профиль персоны (см. [раздел 8.5](#)), действия которой явились возможной причиной возникновения рассматриваемого инцидента, а также перейти к сессии (см. [раздел 9.2](#)), во время которой произошел инцидент.

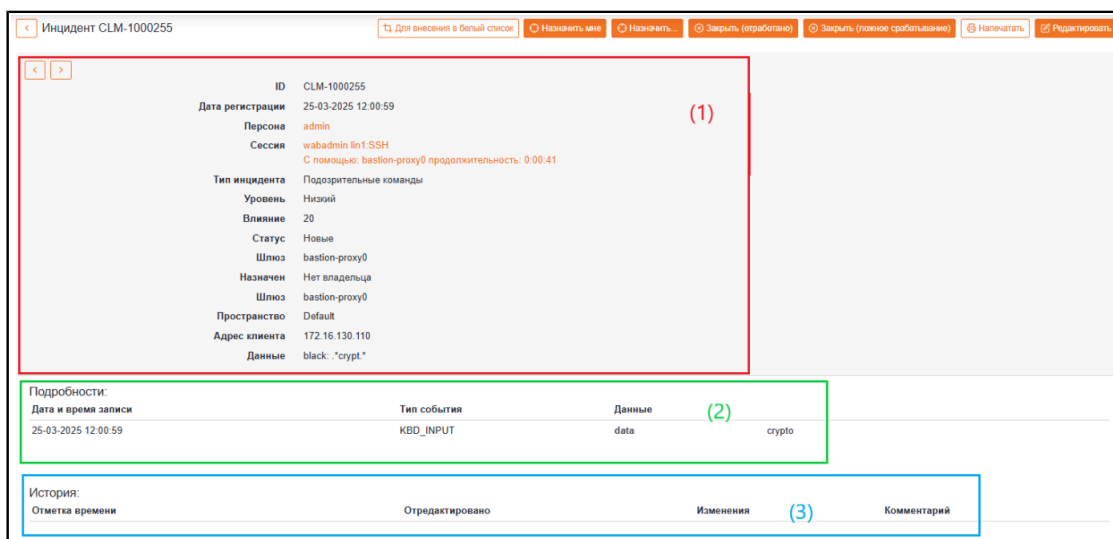


Рисунок 27 – Карточка инцидента

Пользователь может распечатать карточку инцидента, нажав на кнопку **Напечатать**.

10.3 Создать инцидент

Создание инцидента вручную необходимо в следующий случаях:

- событие в сессии не детектируется встроенными детекторами аномалий как инцидент, но в рамках политики для персоны действие является запрещенным;
- событие должно дополнительно контролироваться офицером безопасности.

Для создания инцидента необходимо:

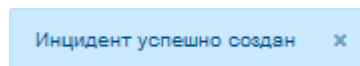
Шаг 1. В профиле пользовательской сессии нажать на кнопку **Создать инцидент**.



Шаг 2. В появившейся форме заполнить необходимые поля

Шаг 3. Сохранить инцидент нажатием на кнопку **Сохранить**.

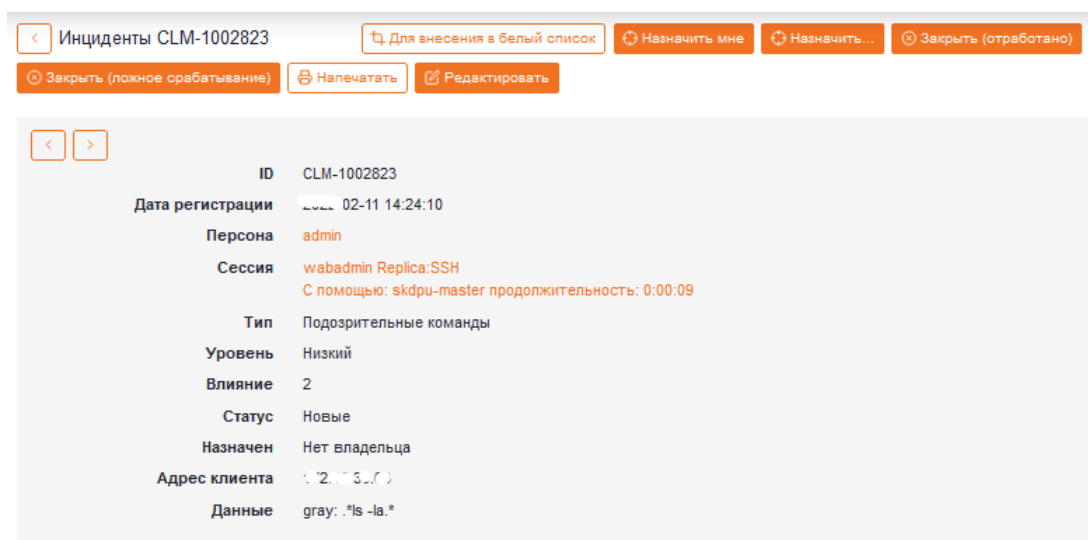
При успешном создании инцидента появится оповещение



10.4 Редактировать инцидент

Для редактирования параметров инцидента необходимо:

Шаг 1. В профиле инцидента нажать на кнопку **Редактировать**.



Шаг 2. В появившейся форме изменить необходимые поля

< Инциденты TF-1001514

ID: TF-1001514
Дата регистрации: 15-05-2023 12:12:20
Персона: mds
Сессия: root win1:RDP
С помощью: wab-7-0-7 продолжительность: 0:00:46
Тип инцидента: Необычное время работы

Уровень
Низкий (1)

Статус
Новые (2)

Причина
Отсутствует (3)

Комментарий
(4)

Назначен
Выберите ответственного (5)

Комментарий для истории
(6)

Сохранить

(1) – уровень критичности инцидента:

- низкий;
- средний;
- высокий;
- критичный.

(2) – текущий статус инцидента:

- новый;
- в работе;
- закрытые (отработанные);
- закрытые (эскалация).

(3) – причина возникновения инцидента:

- отсутствует;
- отработано;
- эскалация;
- требуется обучение персонала;
- требуется изменение политики;
- ложное срабатывание.



Поле **Причина** будет возможно отредактировать только в том случае, когда в профиле инцидента он будет отработан : закрыть (отработано), закрыть (ложное срабатывание) или после изменения статуса, о чем дальше в развернутом виде предоставляются комментарии.

- (4) – комментарий по инциденту (опционально);
- (5) – ответственный за обработку инцидента (опционально);
- (6) – комментарии по вносимым изменениям в описание инцидента (опционально).

Шаг 3. Сохранить инцидент нажатием на кнопку **Сохранить**.

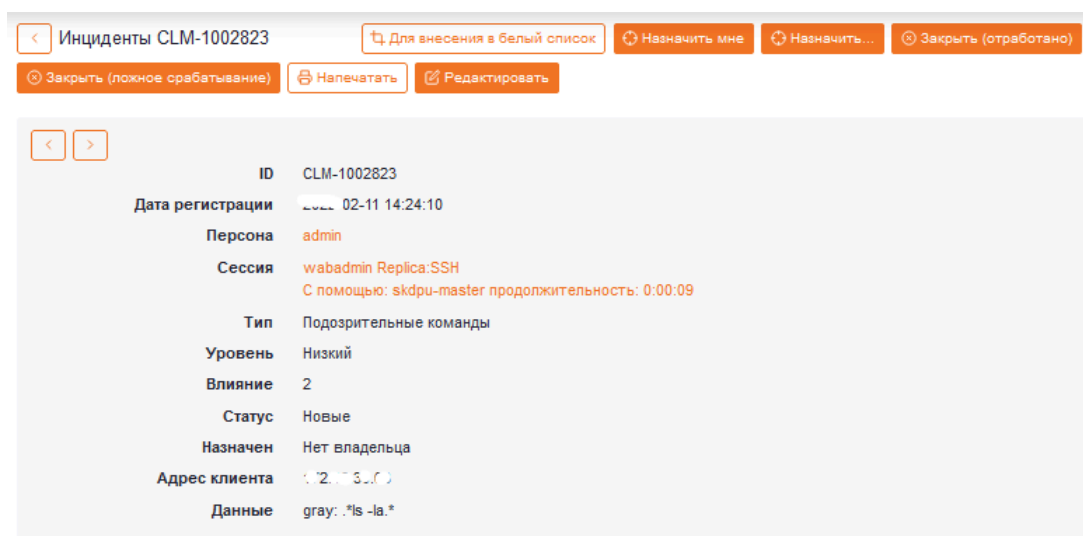
При успешном редактировании инцидента появится оповещение

Данные инцидента обновлены

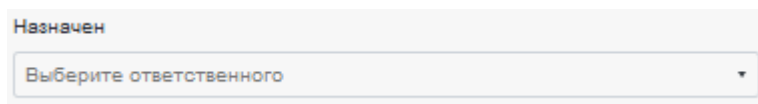
10.5 Назначить ответственного за обработку инцидента

Для назначения ответственного за обработку инцидента необходимо:

Шаг 1. В профиле инцидента нажать на кнопку **Редактировать**.

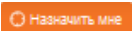



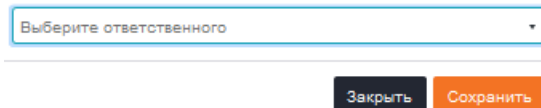
Шаг 2. В появившейся форме (см. [раздел 10.4](#)) выбрать ответственного лицо в поле **Назначен**




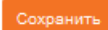
В списке пользователей, которых можно выбрать как ответственных за инцидент, будут только те пользователи, у которых есть право на работы с инцидентами.



Также предоставляется возможность назначить ответственным за обработку инцидента непосредственно в профиле инцидента себя (нажатием на кнопку ) или другое лицо (нажатием на кнопку ). В случае назначения другого лица необходимо выбрать его в появившейся форме

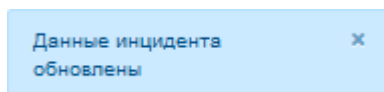


Выберите ответственного


Шаг 3. Сохранить инцидент нажатием на кнопку  .

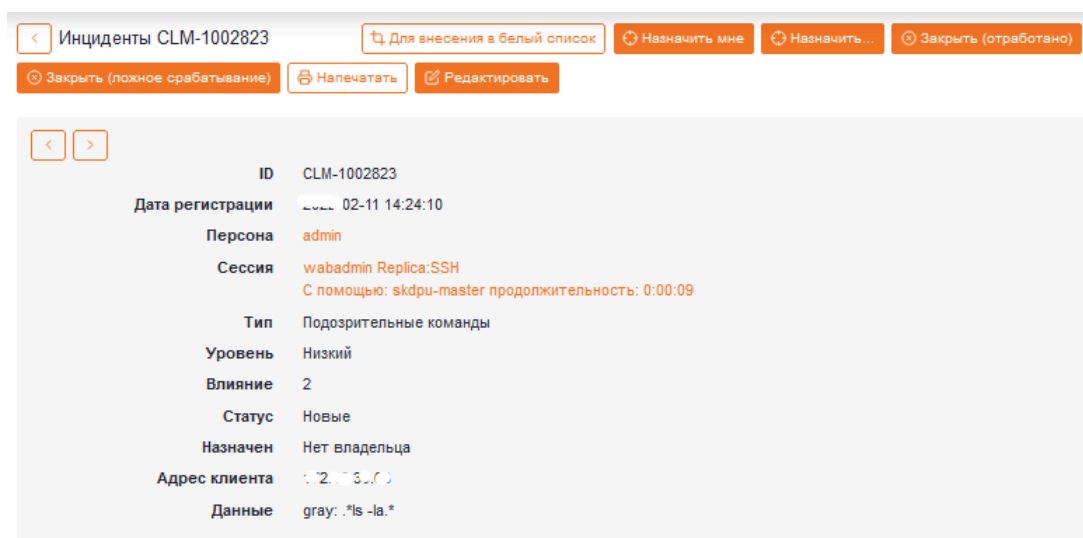
При успешном редактировании инцидента появится оповещение



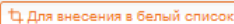
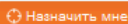
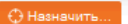
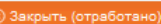
10.6 Закрывать инцидент




Для закрытия инцидента необходимо:

Шаг 1. В профиле инцидента нажать на кнопку  .



Инциденты CLM-1002823

ID	CLM-1002823
Дата регистрации	2022-02-11 14:24:10
Персона	admin
Сессия	wabadmin Replica:SSH С помощью: skdpu-master продолжительность: 0:00:09
Тип	Подозрительные команды
Уровень	Низкий
Влияние	2
Статус	Новые
Назначен	Нет владельца
Адрес клиента	192.168.3.10
Данные	gray: *ls -la.*

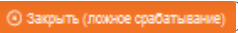

Шаг 2. В появившейся форме (см. [раздел 10.4](#)) выбрать статус инцидента **Закрытие** в поле **Статус**



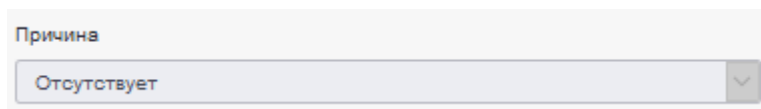
Статус

Новые



Также предоставляется возможность закрывать инциденты непосредственно в профиле инцидента в случае ложного срабатывания (нажатием на кнопку ) или в случае окончания обработки инцидента (нажатием на кнопку ). В зависимости от выбранного варианта закрытия инцидента автоматически указывается причина его возникновения и меняется статус.

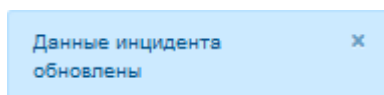
Шаг 3. В поле **Причина** выбрать возможную причину возникновения инцидента




Причина
Отсутствует

Шаг 4. Сохранить инцидент нажатием на кнопку .

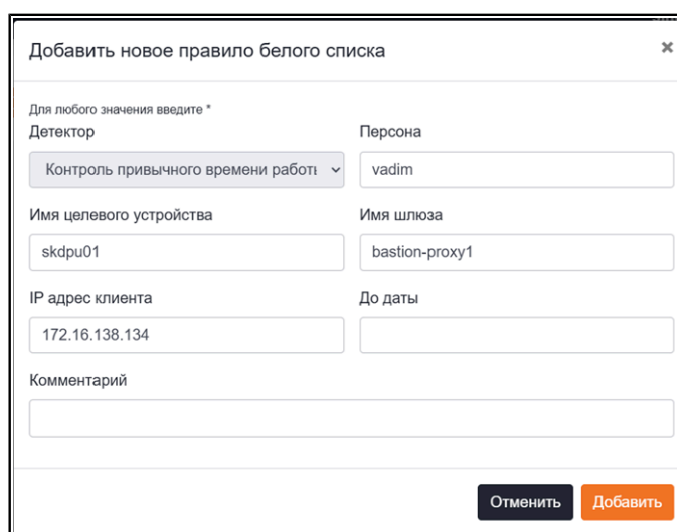
При успешном редактировании инцидента появится оповещение



10.7 Настройка правил белого списка инцидентов

Чтобы настроить правила необходимо в разделе **Инциденты** перейти в карточку инцидента (подробнее см. [раздел 10.2](#)). Для добавления нового правила необходимо нажать на кнопку **Для внесения в белый список** .

В появившейся форме ввести дату, до которой будет действовать правило и комментарий по необходимости. Остальные поля заполняются автоматически исходя из данных в карточке инцидента.



Добавить новое правило белого списка

Для любого значения введите *

Детектор	Персона
Контроль привычного времени работ	vadim
Имя целевого устройства	Имя шлюза
skdru01	bastion-proxy1
IP адрес клиента	До даты
172.16.138.134	
Комментарий	

Отменить Добавить

Рисунок 28 – Добавление правила белого списка из инцидента

При успешном добавлении правила появляется оповещение

Создано новое правило белого списка ✕

11 КОМПОНЕНТЫ

11.1 Общие сведения

СКДПУ НТ получает информацию о персонах, а также данные пользовательских сессий, которые поступают в СКДПУ НТ от шлюзов доступа.


В разделе веб-интерфейса **Компоненты** представлены несколько разделов:

- раздел **Шлюзы** с перечнем систем, которые имеют подключение к СКДПУ НТ и предоставляют данные для анализа;
- раздел **Цели** с перечнем целевых устройств целевой инфраструктуры, к которым осуществляли доступ персоны. По каждому из целевых устройств пользователь СКДПУ НТ может получить статистику использования;
- раздел **Адреса клиента** с перечнем IP-адресов устройств, которые используют пользователи шлюзов (персоны) при входе на шлюзы.

11.2 Шлюзы


В данном разделе перечислены шлюзы доступа, с которых есть зарегистрированные сессии в СКДПУ НТ и данные пользовательских сессий целевых систем (см. [рисунок 29](#)).




Рисунок 29 – Раздел **Компоненты** > **Шлюзы**


 Изменить параметры подключения к шлюзам могут только пользователи с правами администратора.

СКДПУ НТ предоставляет информацию о шлюзах, включающую следующие данные:

- (1) – идентификатор шлюза;
- (2) – URL шлюза;
- (3) – тип шлюза;
- (4) – дата и время последнего использования;
- (5) – статус соединения.

 Возможны следующие состояния:

- Соединение установлено 
- Ошибка соединения 
- Аутентификационные данные не были введены 

Пользователь может распечатать список шлюзов, нажав на кнопку .

Для перехода в карточку шлюза необходимо нажать на нужную строку, после чего появится более детальная информация (см. [рисунок 30](#)).

Компоненты farm-master:	
Тип шлюза	Bastion
Адрес	https://10.5.45.50
Имя пользователя	admin
Пароль	задан
Ключ API	задан
Пространство	Default
Время последнего использования	15-04-2025 15:28:09

Рисунок 30 – Карточка шлюза

Пространство является дополнительным маркером шлюза, который устанавливается администратором СКДПУ НТ для однозначного различения объектов обработки и сессий, приходящих с данного шлюза. Пространство *default* задается шлюзу автоматически при первом появлении шлюза в СКДПУ НТ.

При отсутствии данных о пароле или API-ключе в таблице выводится статус **Данные не введены**.

В карточке шлюза возможно быстро проверить статус соединения, нажав на кнопку

 , или напечатать, нажав на кнопку .

Шлюзы могут быть объединены в группы для настроек конфигурации администратором системы.

11.3 Цели

В рассматриваемом разделе перечислены целевые устройства, к которым осуществляли доступ персоны через соответствующий шлюз доступа (см. [рисунок 31](#)).

(1)	(2)	(3)	(4)	(5)
Имя устройства	IP-адрес цели	Пространство	Сервис	Время последнего использования
betatarget1	10.5.45.50	Default	☆ RDP	15-04-2025 10:59:40
betatarget1	10.5.45.20	Default	☆ SSH	15-04-2025 10:59:32
alphatarget1	10.5.45.10	Default	☆ SSH	15-04-2025 11:52:42
alphatarget1	10.5.45.10	Default	☆ RDP	15-04-2025 16:21:10
alphatarget1	10.5.45.10	Default	☆ RDP	15-04-2025 16:20:31

Рисунок 31 – Раздел **Компоненты > Цели**

- (1) – имя устройства;
- (2) – IP-адрес цели;
- (3) – пространство, назначенное соответствующему шлюзу доступа, через которое происходит подключение к целевому устройству;
- (4) – тип подключения;
- (5) – время и дата последнего использования.

При нажатии на кнопку **Добавить фильтры** появляется дополнительное поле, в котором можно выбрать **Имя устройства** и **Сервис**, где будет задана дополнительная маска для более удобного поиска.

Кнопкой **☆** можно добавить цель в избранное для более удобного доступа к просмотру, а также отслеживанием на главной странице **Мониторинга**.

Пользователь может распечатать список целевых устройств, нажав на кнопку **Напечатать**.

Пользователь может отыскать конкретное целевое устройство, указав ее имя или часть в поле **Поиск**.

Пользователь СКДПУ НТ имеет возможность выбрать целевое устройство для ознакомления с информацией параметрах подключения (1), а также ознакомиться с графическим представлением сессий и инцидентов (2) (см. [рисунок 32](#)).

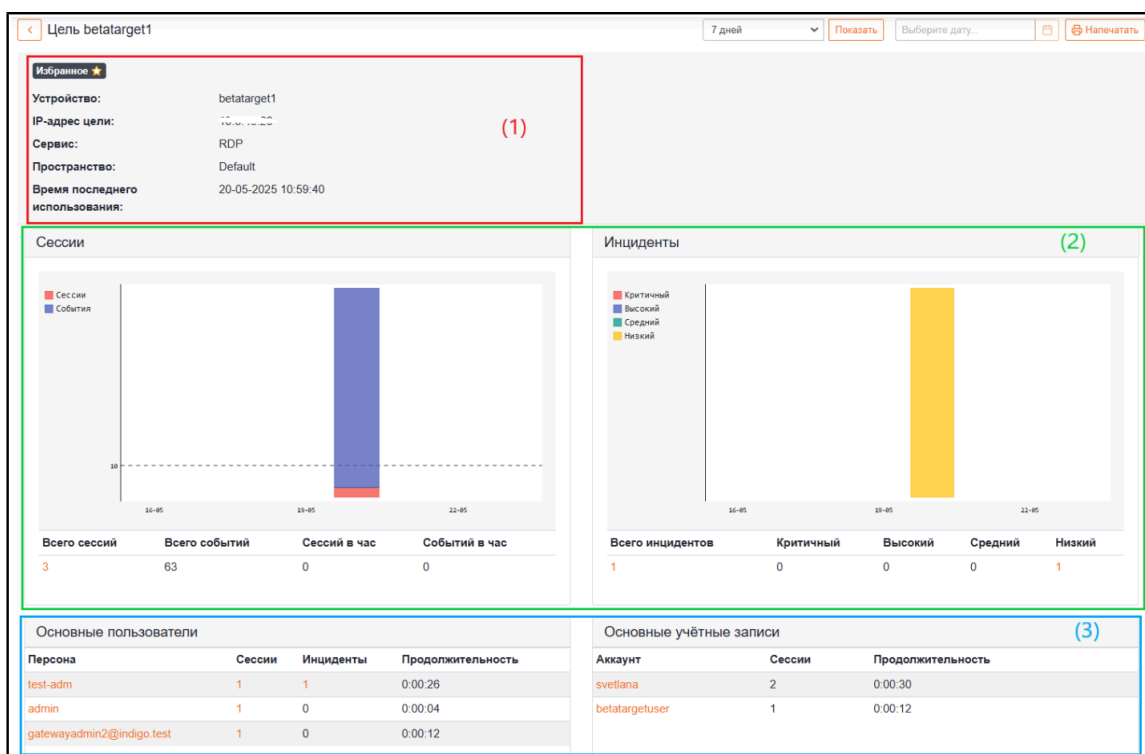


Рисунок 32 – Статистика устройства


Кроме того, пользователь может получить подробную статистику использования выбранного целевого устройства за выбранный временной промежуток, например данные по персонам, которые получали доступ к целевому устройству, данные по сессиям подключения и т.д. (3).

В СКДПУ НТ имеется возможность получить статистические данные за определенный временной промежуток в соответствии с выбранными значениями.

Для выбора доступны следующие временные промежутки:

- за текущий день;
- за предыдущий день;
- за последние семь дней;
- за последний тридцать один день.

Подтверждение осуществляется нажатием на кнопку .

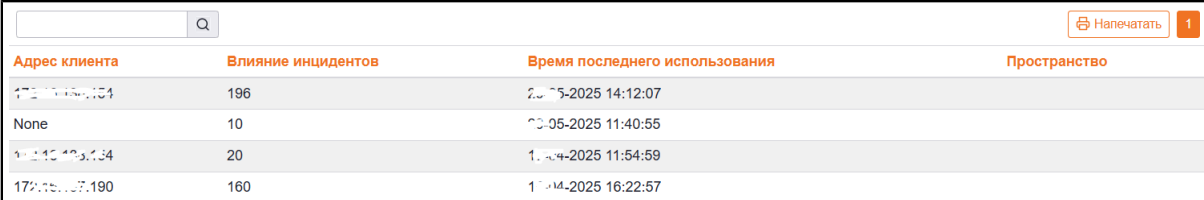
Также пользователь имеет возможность выбрать для просмотра конкретную дату, подтвердив нажатием на кнопку .

Пользователь может оперативно напечатать сводную статистику за выбранный ранее временной промежуток, нажав на кнопку .

При наличии прав на просмотр пользователь СКДПУ НТ имеет возможность перейти в соответствующие разделы для более подробного анализа данных, выбрав активные ссылки, выделенные цветом.

11.4 Адреса клиента

В рассматриваемом разделе перечислены IP-адреса устройств, которые используют пользователи шлюзов (персоны) при входе на целевые устройства. Для каждого адреса указан коэффициент влияния инцидентов и время последнего использования (см. [рисунок 33](#)).



Адрес клиента	Влияние инцидентов	Время последнего использования	Пространство
172.16.1.104	196	2025-05-20 14:12:07	
None	10	2025-05-20 11:40:55	
172.16.1.104	20	2025-05-11 11:54:59	
172.16.1.190	160	2025-05-11 16:22:57	

Рисунок 33 – Раздел **Компоненты > Адреса клиентов**

При помощи поиска можно сузить диапазон выводимых данных для более удобной навигации.

Пользователь СКДПУ НТ в зависимости от настроек доступа имеет возможность выбрать адрес клиента для ознакомления с информацией о времени последнего подключения, а также ознакомиться с графическим представлением сессий и инцидентов (см. [рисунок 34](#)).

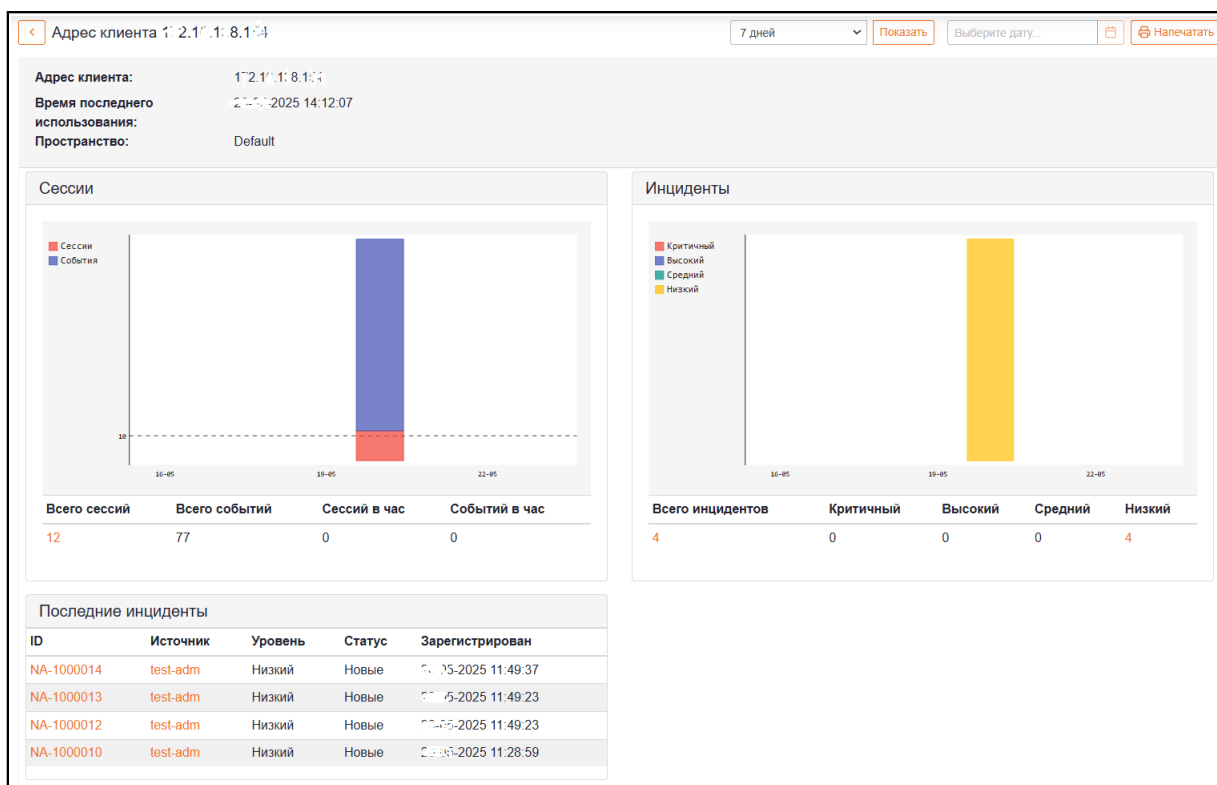


Рисунок 34 – Адрес клиента

Кроме того, можно более детально ознакомиться с зафиксированными инцидентами, перейдя по соответствующим ссылкам.

В СКДПУ НТ имеется возможность получить статистические данные за определенный временной промежуток в соответствии с выбранными значениями.

Для выбора доступны следующие временные промежутки:

- за текущий день;
- за предыдущий день;
- за последние семь дней;
- за последний тридцать один день.

Подтверждение осуществляется нажатием на кнопку **Показать**.

Также пользователь имеет возможность выбрать для просмотра конкретную дату, подтвердив нажатием на кнопку **📅**.

Пользователь может оперативно напечатать сводную статистику за выбранный ранее временной промежуток, нажав на кнопку **Напечатать**.

При наличии прав на просмотр пользователь СКДПУ НТ имеет возможность перейти в соответствующие разделы для более подробного анализа данных, выбрав активные ссылки, выделенные цветом.

Приложение

А

ОПИСАНИЕ ИНЦИДЕНТОВ

Тип инцидента	Описание
Подозрительные команды	Инцидент возникает, если при анализе команд в пользовательских сессиях детектируются фрагменты слов, команд, адресов, содержащихся в "черном" (black) или "сером" (grey) списках. Названия соответствуют уровню нежелательности команд или их частей. Для каждого списка установлено свое значение фактора.
Разрыв сессии	Инцидент создается, если происходит принудительное закрытие пользовательских сессий на целевых системах при обнаружении команд из черных списков, заданных в политике безопасности шлюзов доступа.
Необычное время работы	Инцидент возникает, если начало сессии выпадает на нетипичный для персоны интервал времени. Для этого должно пройти достаточно времени для отслеживания подсистемой Мониторинга и аналитики и анализа на "нетипичность", период накопления данных устанавливается в настройках анализатора.
Уровень доверия	Инцидент создается при переходе уровня доверия вниз через установленную границу (LOW, MEDIUM, HIGH, CRITICAL).
Необычные команды	Инцидент создается, если наблюдается серьезное отклонение от ранее зафиксированного потока команд, который был определен в рамках обучения за указанный период. Анализируется поток команд, которые обычно использует персона (в максимально абстрактном виде). На основе результата анализа формируется профиль базового поведения персоны.
Сетевое расположение	Инцидент создается при использовании для входа нетипичного сетевого адреса (вход не из той подсети). В настройке анализатора можно задать период, в течение которого он не реагирует на новые адреса для новых персон, а собирает типичные сетевые адреса.
Наименее эффективное использование времени сессии	Инцидент создается при падении значения показателя эффективности сессий. Анализируется динамика показателя эффективности сессий персоны.

Тип инцидента	Описание
Индикаторы взрывной активности	Инцидент возникает при повышении типичной активности. В разрезе дня и сессии одновременно анализируются такие активности персоны, как: количество подключений (только в разрезе дня), количество событий, количество и объем полученных или отправленных данных.
Новый доступ	Инцидент создается, если по окончании формирования профиля персона использует новый аккаунт или сервис на привычной целевой системе, или совершает вход на новую целевую систему. (Анализатор сохраняет в профиле персоны информацию о целевых системах, аккаунтах и сервисах, которыми она обычно пользуется.) В настройках анализатора можно задать период накопления данных в профиле, в течение которого он не реагирует на новые доступы.
Недостаток прав	Инцидент создается в случае попытки доступа к файлам или каталогам с недостаточными правами. Детектор отслеживает сеансы передачи файлов по протоколу SFTP .
Туннели и прыжки	Инциденты создаются при использовании персоной средств удаленного доступа (создание туннелей или совершение прыжков). Реагирование происходит не на каждое событие, а при накоплении за день определенного количества. Разному количеству зафиксированных событий соответствуют разные уровни критичности инцидентов.
Прямой логин	Инцидент генерируется при обнаружении удаленного доступа к целевой системе, который осуществляется в обход Шлюзов доступа. Детектор позволяет сигнализировать о доступе к целевым системам на основании данных, получаемых от анализаторов сетевых потоков других производителей. Информацию для анализа предоставляют системы, подключенные в качестве внешних источников обогащения в разделе Настройки > Внешние источники обогащения .
Ошибка аутентификации	Инциденты создаются на первую ошибку и каждую пятую ошибку аутентификации персоны с повышением уровня критичности инцидента. Подсчитывается количество ошибок аутентификации персоны в течение каждого часа.
Забытая персона	Инцидент создается при появлении активности персоны после ее длительного отсутствия (долгое время не было сессий). Уровень критичности инцидента зависит от длительности отсутствия персоны.

Тип инцидента	Описание
Количество переданных файлов	Инцидент создается при превышении порогового значения количества загруженных (downloaded) файлов. Уровень критичности инцидента зависит от количества загруженных данных.
Сканеры	Инцидент создается при фиксации множественных попыток доступа без дальнейшей авторизации на целевую систему от конкретного источника в течение короткого времени.
КО. Удаление устройства.	Инцидент возникает при удалении оператором шлюза целевого устройства в политике шлюза при нахождении в Кабинете оператора. При этом само целевое устройство не удаляется со шлюза, а указывается в свойствах инцидента для дальнейших действий.
КО. Создание устройства	Инцидент возникает, когда оператор шлюза пытается добавить целевое устройство в политику шлюза с именем, которое уже существует в списке устройств на шлюзе или в сохраненных у другого пользователя Кабинета оператора. Не обязательно видно текущему оператору шлюза в его перечне устройств.
КО. Создание аккаунта	Инцидент возникает, когда оператор шлюза пытается добавить на целевое устройство в политике шлюза аккаунт, который уже существует на нем.
КО. Применение политики	Инцидент возникает при любых ошибках применения политики на шлюзе (выполнения событий в журнале).

Приложение

Б

ОПИСАНИЕ ОТЧЕТОВ

Общие отчеты по системам

Обобщённая справка

Отчет содержит сводную информацию за выбранный период и за предыдущий период, по длительности равный выбранному периоду, а также численное сравнение показателей.

Учётные записи на целевых системах

Отчет содержит информацию за выбранный период о том, под какими учетными записями производился вход на целевые устройства, сколько сессий было совершено под каждой учетной записью, сколько инцидентов было зафиксировано (с разбивкой по уровню критичности и размеру влияния).



Отчет "Наиболее часто используемые целевые учётные записи" отличается от "Обзорного отчета по сессиям" тем, что в первом по умолчанию записи будут сгруппированы по имени учетной записи на целевом устройстве, а во втором группировки по умолчанию не будет.

Наиболее часто используемые целевые учётные записи

Отчет содержит информацию о том, какие учетные записи на целевых устройствах используются наиболее часто. Содержание и внешний вид отчета различается в зависимости от выбранного для группировки поля.

Отчет позволяет настроить включение в него только вновь зарегистрированные в выбранном периоде персоны или целевые устройства.

Обзорный отчёт по сессиям

Отчет содержит информацию о сессиях за выбранный период. Содержание и внешний вид отчета различаются в зависимости от выбранного для группировки поля.



"Обзорный отчет по сессиям" отличается от отчета "Наиболее часто используемые целевые учётные записи" тем, что во втором по умолчанию записи будут сгруппированы по имени учетной записи на целевом устройстве, а в первом группировки по умолчанию не будет.

В отчете можно указать для отбора направление перемещения данных: загрузка или скачивание.

Отчет позволяет настроить включение в него только вновь зарегистрированные в выбранном периоде персоны или целевые устройства.

Обзорный отчёт по учётным записям

Отчет содержит информацию за выбранный период о том, под какими учетными записями производился вход на целевые устройства, сколько сессий было совершено под каждой учетной записью, сколько инцидентов было зафиксировано (с разбивкой по уровню критичности и размеру влияния).

Для отчета можно задать **Максимальное количество записей**, то есть строк в таблице вывода и **Максимальное количество устройств** для одной персоны.

Отчеты по текущей активности

Новые сессии

Отчет содержит информацию о сессиях, которые были совершены за выбранный период. Поскольку форма отчета позволяет выбрать только ближайший период (различные временные интервалы в пределах текущих и предыдущих суток), то в отчете будут выведены только новые сессии.

В отчете можно указать для отбора направление перемещения данных: загрузка или скачивание.

Отчет позволяет настроить включение в него только вновь зарегистрированные в выбранном периоде персоны или целевые устройства.

Отчет позволяет отобразить сессии, которые открыты на момент формирования отчета, если установлен флаг **Выводить только открытые сессии**. По умолчанию флаг не установлен.

Целевые системы в использовании

Отчет содержит информацию за выбранный период об использовании целевых устройств: когда в последний раз и с помощью какого типа сервиса был осуществлен доступ.

Отчеты по использованию

Общий отчет по ситуации

Отчет содержит сводную информацию за выбранный период и за предыдущий период, по длительности равный выбранному периоду, а также численное сравнение показателей.

Наиболее активные персоны

Отчет содержит информацию о Персонах с наибольшими показателями активности по данным подсистемы для выбранного периода времени.

Наименее активные персоны

Отчет содержит информацию о Персонах с минимальными показателями активности по данным подсистемы, в том числе и Персоны без зарегистрированной активности для выбранного периода времени.

Наиболее длительные сессии

Отчет содержит информацию о наиболее длительных по времени сессий для заданного периода времени и прочих ограничений.

Наиболее долго работающие персоны

Отчет содержит информацию о Персонах, для которых зарегистрировано наиболее длительная активная работа в рамках сессий для заданного периода времени и прочих ограничений.

Наиболее занятые целевые системы

Отчет содержит список целевых систем, на которые зарегистрировано наибольшее количество сессий для заданного периода времени.

Краткосрочные сеансы

Отчет содержит сведения по сессиям с минимальной длительностью для заданного периода времени.

Обзор по шлюзам

Отчет содержит сводные показатели с разбиением по каждому активному шлюзу за период. Показатели включают в себя сведения о количестве сессий, наиболее активных персонах, наиболее активно используемых целевых системах и инцидентах.

Обзор по целевой системе

Отчет содержит сводные показатели по указанной целевой системе за заданный период. Показатели включают в себя сведения о количестве сессий, наиболее активных персонах и другие.

Целевые учётные записи

Отчет содержит список целевых систем и учетных записей по активности за заданный период.

Новые персоны в системе

В результате выполнения отчета будет выдан список профилей Персон, которые были зарегистрированы подсистемой за указанный период времени, а также дополнительные данные по данным Персонам.

Новые целевые системы

В результате выполнения отчета будет выдан список профилей целевых систем, на которые впервые была зарегистрирована активность по данным подсистемы.

Неиспользуемые системы

Отчет позволяет получить список целевых систем, на которых не регистрировалась активность пользователей за указанный период времени.

Неиспользуемые целевые учётные записи

Отчет позволяет получить список целевых учетных записей, которые известны в подсистеме, но за указанный период времени активность на них не регистрировалась.

Наименее эффективное использование времени сессии

Подсистема при анализе активностей пользователей учитывает количество событий в рамках сессии, зарегистрированную длительность, а также наличие значительных промежутков в рамках каждой сессии между отдельными событиями. Соотношение длительности и распределения активностей пользователя в рамках сессии вычисляется как показатель эффективности в сессии. Данный отчет позволяет получить список сессий или активных Персон, для которых показатель эффективности был рассчитан минимальный.

Максимальное число параллельных сессий за период

С помощью этого отчета возможно определить нагрузку на лицензионные ограничения для шлюзов. Отчет по каждому шлюзу выдает максимальное количество параллельных сессий за указанный период, а также максимальное количество параллельных сессий, зарегистрированных подсистемой по доступным данным.

Отчеты по безопасности

Использование УЗ по умолчанию

Отчет позволяет получить список сессий, где в качестве целевой учетной записи использовались стандартные учетные записи администраторов ("Администратор", "root" и т.п.).

Ошибки авторизации

Отчет позволяет получить данные по инцидентам типа "Ошибка авторизации", как в виде списка сессий, так и в других представлениях.

Потенциально опасные приложения

Отчет позволяет получить данные по инцидентам, вызванным нахождением команд из черного и серого списка.

Использование Jump серверов

Отчет позволяет получить сведения об инцидентах типа "туннели и прыжки", когда операторы используют команды удаленного доступа внутри наблюдаемой сессии.

Неожиданные команды

Отчет позволяет получить сведения об инцидентах типа "Нехарактерные команды", когда подсистема обнаруживает для пользователей факты использования команд, которые ранее эти пользователи не использовали по данным подсистемы. Значительно изменение поведения пользователей может быть признаком компроментации учетной записи.

Неожиданное время работы

Отчет позволяет получить сведения об инцидентах типа "Нехарактерное время работы", когда подсистема обнаруживает для пользователей факты активности в периоды времени, которые обычно данный пользователь не использует. Нарушение стандартного времени работы для пользователя может быть признаком компроментации учетной записи.

Принудительно закрытые сессии

Отчет позволяет получить сведения об инцидентах типа "Принудительное закрытие сессии администратором шлюза", когда сессия удаленного доступа принудительно завершается по команде администратора безопасности или правилам реагирования.

Контроль изменения уровня доверия

Отчет позволяет получить сведения об инцидентах типа "Уровень доверия". Подсистема для каждой персоны вычисляет показатель "уровень доверия", который стремится к определенному значению в среднем. Каждый инцидент уменьшает уровень доверия персоны. При отсутствии инцидентов уровень доверия персоны постепенно восстанавливается. Снижение уровня доверия может означать множественные сработки инцидентов для персоны. Значительное снижение уровня доверия в моменте может являться признаком компроментации учетной записи пользователя.

Детектирование потенциально опасных команд

Отчет позволяет получить сведения по инцидентам, вызванным нахождением команд из черного и серого списка.

Забытая персона

Отчет позволяет получить список персон, для которых зарегистрирована активность после долгого периода неактивности за указанный период.

Количество переданных файлов

Отчет позволяет получить сведения о событиях объемной передачи файлов или передачи большого количества файлов.

Индикаторы взрывной активности

Отчет позволяет получить сведения о ситуациях, когда пользователи проявляли нехарактерную активность в численных показателях: очень большое количество сессий, очень большое количество

передаваемых файлов, очень большие объемы передаваемых файлов по сравнению с известными показателями данных пользователей.

Сканеры

Отчет позволяет получить сведения о ситуациях внешних соединений со шлюзами удаленного доступа, за которыми не следовало успешной авторизации и штатной пользовательской активности. Обычно заметная активность такого рода означает активность легитимных и вредоносных сетевых сканеров.

Инциденты

Новые инциденты

Отчет позволяет получить сведения об инцидентах со статусом "новый".

Инциденты без ответственного

Отчет позволяет получить сведения об инцидентах без явно определенного ответственного.

Основные нарушители

Отчет позволяет получить сведения о персонах с наибольшим количеством и влиянием инцидентов.

Инциденты в работе

Отчет позволяет получить сведения об открытых инцидентах, для которых есть изменения.

Мои инциденты

Отчет позволяет получить сведения об инцидентах, назначенных на текущего активного пользователя.

Закрытые инциденты

Отчет позволяет получить сведения об инцидентах за заданный период времени со статусом "закрыто".

Наиболее критичные инциденты по персонам

Отчет позволяет получить сведения о персонах и их наиболее критичных инцидентах за заданный период времени.

Целевые системы с высоким риском

Отчет позволяет получить список целевых систем, для которых зарегистрировано наибольшее количество инцидентов.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

API	Application Programming Interface — описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой.
CSV	Comma-Separated Values — текстовый формат, предназначенный для представления табличных данных.
DAR	Data Access Restrictions — ограничение доступа к данным архива пользовательских сессий
HTTP	HyperText Transfer Protocol — протокол передачи гипертекста.
IP	Internet Protocol (межсетевой протокол) — маршрутизируемый протокол сетевого уровня стека TCP/IP.
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к каталогам) — протокол прикладного уровня для доступа к службе каталогов X.500
RADIUS	RADIUS (Remote Authentication in Dial-In User Service) — протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием.
RDP	Remote Desktop Protocol — протокол удаленного рабочего стола
RLOGIN	Remote LOGIN — удалённый вход в систему.
SCP	Secure Copy Protocol — утилита и протокол копирования файлов между компьютерами, использующий, в отличие от утилиты RCP, в качестве транспорта не RSH, а зашифрованный SSH.
SFTP	SSH File Transfer Protocol — протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения.
SSH	Secure SHell (безопасная оболочка) — протокол защищенной передачи данных.
TELNET	TErminaL NETwork — сетевой протокол для реализации текстового интерфейса по сети (при помощи транспорта TCP).
TLS	Transport Layer Security — протокол защиты транспортного уровня
TOTP	Time-based One-Time Password Algorithm — алгоритм создания одноразовых паролей для защищённой аутентификации, являющийся улучшением HOTP. Является алгоритмом односторонней аутентификации — сервер удостоверяется в подлинности клиента.
URL	Uniform Resource Locator (унифицированный указатель ресурса) — система унифицированных адресов электронных ресурсов.

АРМ Автоматизированное рабочее место

ПО Программное обеспечение

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 – Ошибка входа.....	9
Рисунок 2 – Интерфейс СКДПУ НТ.....	10
Рисунок 3 – Раздел Мониторинг.....	14
Рисунок 4 – Самые продолжительные сессии.....	15
Рисунок 5 – Активность пользователей.....	16
Рисунок 6 – Инциденты.....	17
Рисунок 7 – Основные нарушители.....	17
Рисунок 8 – Основные инциденты.....	18
Рисунок 9 – Статистика.....	18
Рисунок 10 – Активные пользователи.....	19
Рисунок 11 – Активные пользователи под наблюдением.....	19
Рисунок 12 – Активность целей.....	20
Рисунок 13 – Раздел Отчеты Отчеты.....	23
Рисунок 14 – Пример группировки и сортировки в отчете.....	27
Рисунок 15 – Раздел Отчеты История выполнения.....	28
Рисунок 16 – Раздел Отчеты Профили выполнения.....	29
Рисунок 17 – Раздел Персоны.....	33
Рисунок 18 – Фильтр пользователей по тегам.....	34
Рисунок 19 – Цифровой профиль пользователя - уровень доверия.....	35
Рисунок 20 – Цифровой профиль пользователя.....	37
Рисунок 21 – Управление персонками (склеивание и забывание).....	37
Рисунок 22 – Страница Сессии.....	41
Рисунок 23 – Пример выборки сессий.....	42
Рисунок 24 – Карточка пользовательской сессии.....	44
Рисунок 25 – Раздел Инциденты.....	47
Рисунок 26 – Пример представления результатов выборки всех инцидентов.....	48
Рисунок 27 – Карточка инцидента.....	49
Рисунок 28 – Добавление правила белого списка из инцидента.....	54
Рисунок 29 – Раздел Компоненты Шлюзы.....	56
Рисунок 30 – Карточка шлюза.....	57
Рисунок 31 – Раздел Компоненты Цели.....	57
Рисунок 32 – Статистика устройства.....	58
Рисунок 33 – Раздел Компоненты Адреса клиентов.....	59
Рисунок 34 – Адрес клиента.....	60

ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1 – Минимальные характеристики аппаратно-программного обеспечения АРМ пользователя СКДПУ НТ.....	7
---	---

