



**ПРОГРАММНЫЙ КОМПЛЕКС
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ
«НОВЫЕ ТЕХНОЛОГИИ»
Версия: 2.1.58**

Руководство пользователя

RU.33654484.0001-01 90 01

Листов 49

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 Мониторинг.....	12
5.1 Самые продолжительные сессии.....	13
5.2 Активность пользователей.....	14
5.3 Инциденты.....	14
5.4 Основные нарушители.....	15
5.5 Основные инциденты.....	15
5.6 Статистика.....	16
5.7 Активные пользователи.....	16
5.8 Активные пользователи под наблюдением.....	16
6 Отчеты.....	18
6.1 Общие сведения.....	18
6.2 Отчеты.....	18
6.2.1 Создание отчета.....	19
6.2.2 Редактирование отчета.....	19
6.2.3 Удаление отчета.....	20
6.2.4 Генерирование отчета.....	20
6.3 Библиотека отчетов.....	21
6.4 История выполнения.....	21
6.4.1 Скачивание отчета.....	22
6.5 Профили выполнения.....	23
6.5.1 Создание профиля выполнения.....	23
6.5.2 Редактирование профиля выполнения.....	24
6.5.3 Удаление профиля выполнения.....	25
7 Персоны.....	27
7.1 Общие сведения.....	27
7.2 Уровень доверия.....	27
7.3 Цифровой профиль пользователя.....	28
8 Сессии.....	30
8.1 Общие сведения.....	30

8.2 Профиль пользовательской сессии.....	31
9 Инциденты.....	33
9.1 Общие сведения.....	33
9.2 Профиль инцидента.....	35
9.3 Создать инцидент.....	36
9.4 Редактировать инцидент.....	36
9.5 Назначить ответственного за обработку инцидента.....	39
9.6 Закрыть инцидент.....	40
10 Компоненты.....	41
10.1 Общие сведения.....	41
10.2 Шлюзы.....	41
10.3 Цели.....	43
Перечень сокращений.....	45
Перечень рисунков.....	47
Перечень таблиц.....	48

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ СКДПУ НТ

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

СКДПУ НТ - устройство в информационной сети с установленным СКДПУ НТ, 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 единая точка 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, SCSI или SATA
Интерфейсы	Интерфейс для подключения к LAN
Монитор	Разрешение экрана при работе с управляющим интерфейсом 1280x1024
Веб-обозреватель	Mozilla Firefox 80.0, Google Chrome 10.0 – 80.0, Microsoft Edge версии 44.18362.449.0. и выше. Обеспечивающий поддержку стандарта HTTP 1.1, TLS 1.2 и лучше
Брокер сообщений	Свободно распространяемый клиент для различных протоколов удаленного доступа, включая SSH, TELNET, RLOGIN. В качестве таких клиентов могут быть использованы «PuTTY», «WinSCP», «FileZilla»

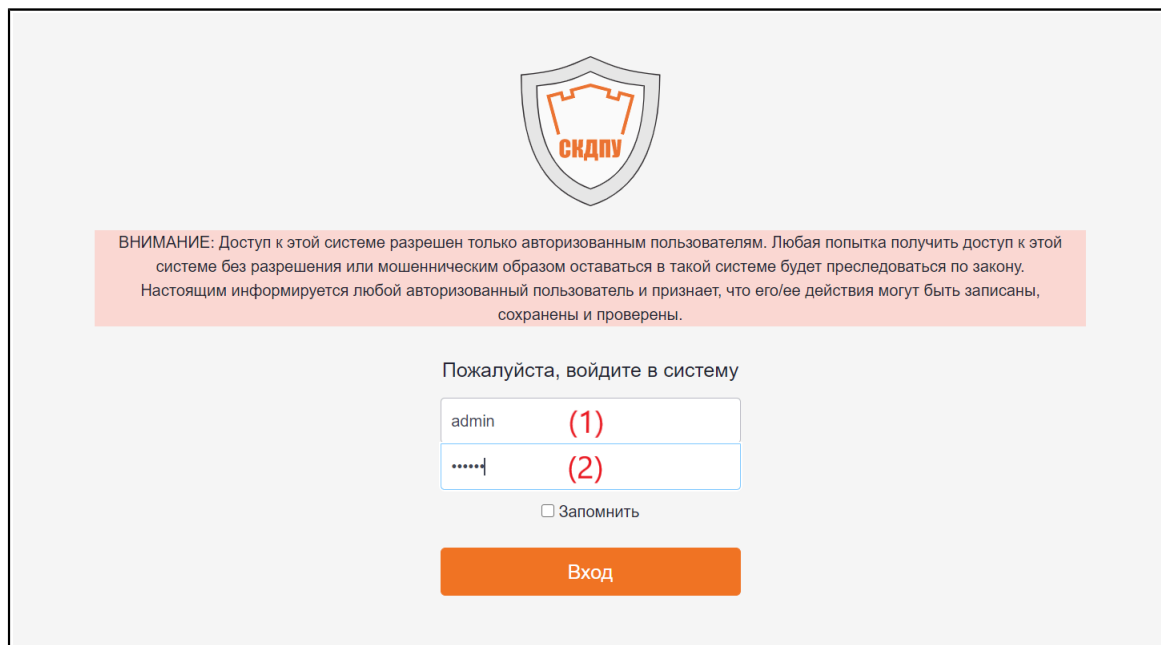
4 НАЧАЛО РАБОТЫ

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)



СКДПУ

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.

Пожалуйста, войдите в систему

admin (1)

..... (2)

Запомнить

Вход

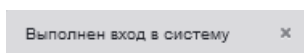
Рисунок 1 – Форма ввода логина и пароля

Шаг 3. Нажать на кнопку  .

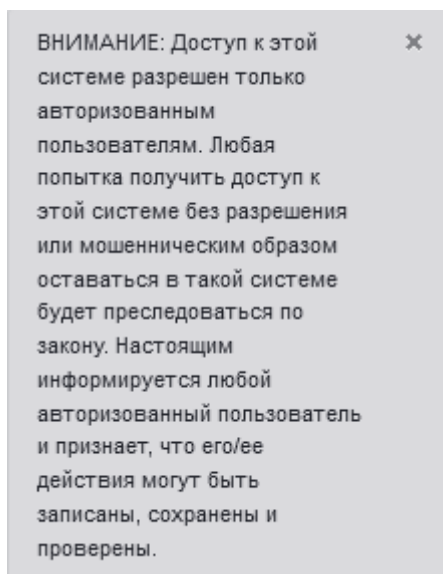
В случае успешной авторизации администратор переходит в раздел веб-интерфейса СКДПУ НТ.

При успешной авторизации в правом нижнем углу появится следующая информация:

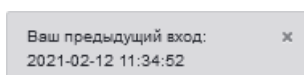
- выполнен вход в систему



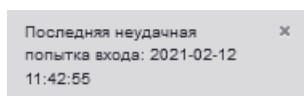
- предупреждение пользователя об ответственности неправомерного использования и мерах защиты, реализованных в СКДПУ НТ



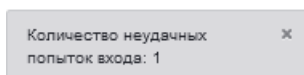
- дата и время предыдущей успешной авторизации



- 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

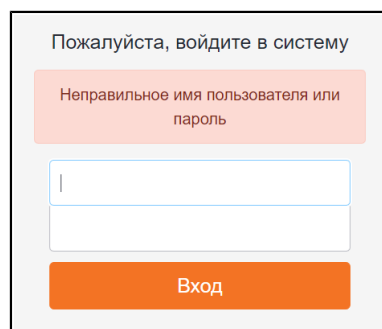


Рисунок 2 – Ошибка входа

4.2 Описание интерфейса

После успешного прохождения процесса идентификации и аутентификации загружается основной интерфейс СКДПУ НТ (см. [рисунок 3](#)).

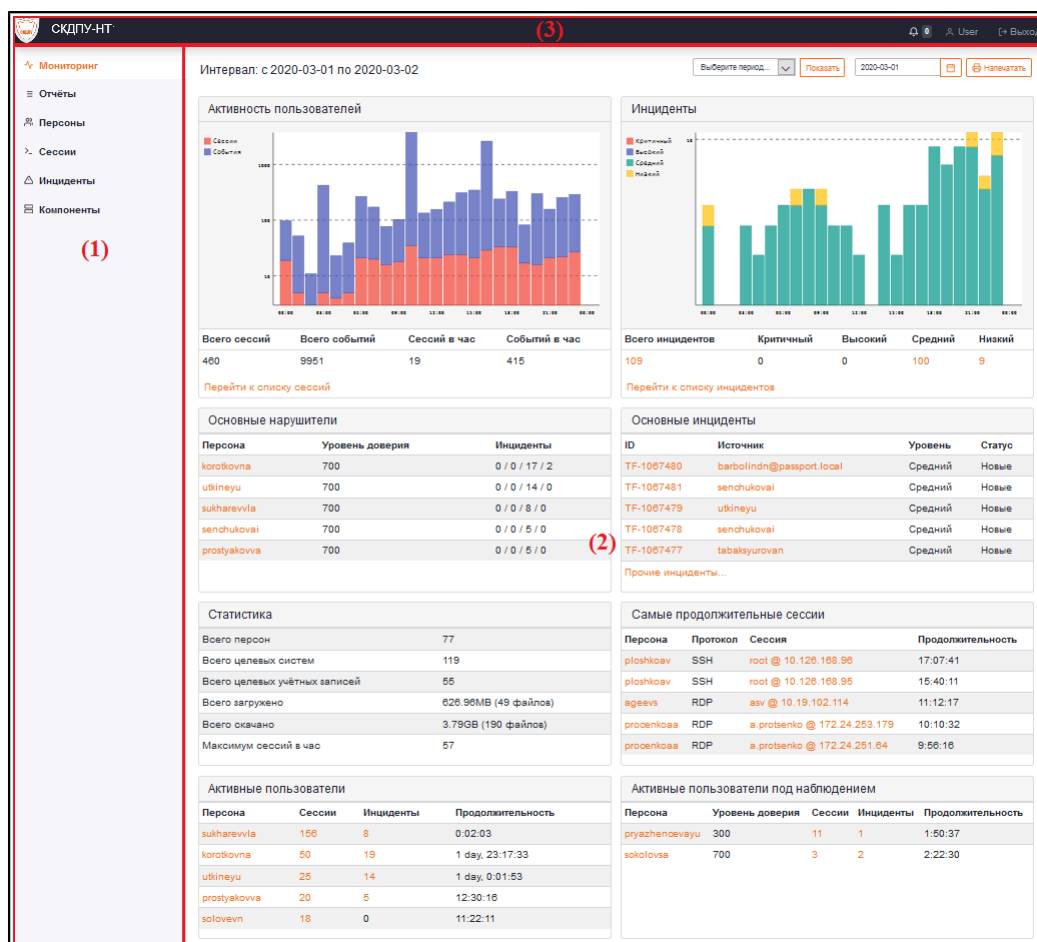


Рисунок 3 – Интерфейс СКДПУ НТ


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




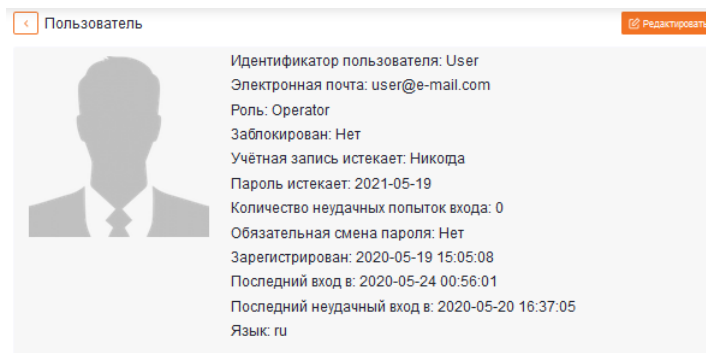
- (1) – логотип и название СКДПУ НТ. При нажатии происходит переход в раздел **Мониторинг**;
- (2) – оповещение о количестве зафиксированных за последнее время инцидентов в пользовательских сессиях целевых систем. При нажатии происходит переход в раздел **Инциденты**;
- (3) – идентификатор текущего пользователя 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.

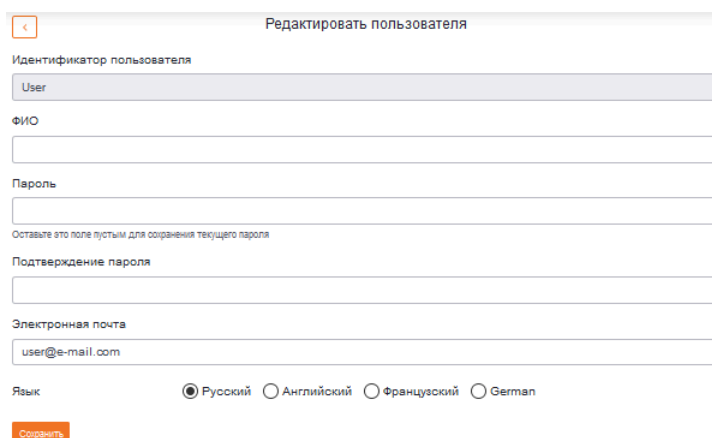
Шаг 2. В открывшейся форме приводятся данные о пользователе, статистика попыток авторизации, сведения о пароле. Далее необходимо нажать на .



Скриншот страницы «Пользователь». Вверху слева — кнопка «<», справа — «Редактировать». В центре — карточка профиля с фото и данными:

- Идентификатор пользователя: User
- Электронная почта: user@e-mail.com
- Роль: Operator
- Заблокирован: Нет
- Учётная запись истекает: Никогда
- Пароль истекает: 2021-05-19
- Количество неудачных попыток входа: 0
- Обязательная смена пароля: Нет
- Зарегистрирован: 2020-05-19 15:05:08
- Последний вход в: 2020-05-24 00:56:01
- Последний неудачный вход в: 2020-05-20 16:37:05
- Язык: ru

Шаг 3. В появившейся форме изменить желаемые данные



Скриншот формы «Редактировать пользователя». Поля для ввода:

- Идентификатор пользователя: User
- ФИО: [пустое поле]
- Пароль: [пустое поле]
- Подтверждение пароля: [пустое поле]
- Электронная почта: user@e-mail.com
- Язык: Русский Английский Французский German

Внизу — кнопка «Сохранить».


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



В случае, если нет необходимости в смене пароля, то поля (2) (3) следует оставить незаполненными.

Шаг 4. Сохранить изменения учетной записи нажатием на .

При успешном сохранении учетной записи появится оповещение

Обновление профиля
пользователя 

5 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 4](#)).

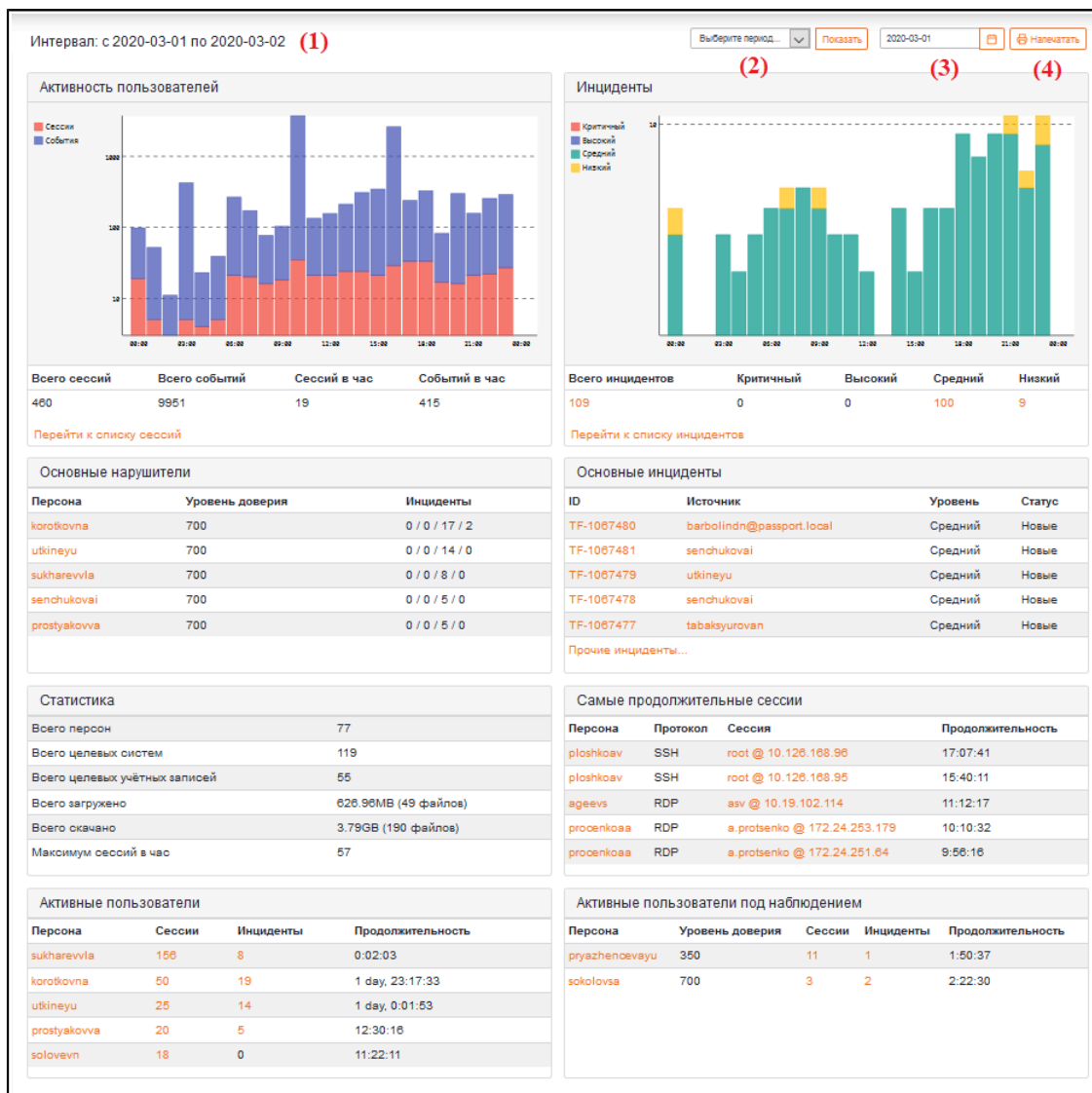



Рисунок 4 – Раздел Мониторинг


Пользователь 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 тридцать один день.

Подтверждение осуществляется нажатием .

Также пользователь имеет возможность выбрать для просмотра конкретную дату, указав ее в (3) и впоследствии подтвердив нажатием .

Пользователь может оперативно напечатать сводную статистику (4) за выбранный ранее временной промежуток, нажав .

При наличии прав на просмотр пользователь 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.

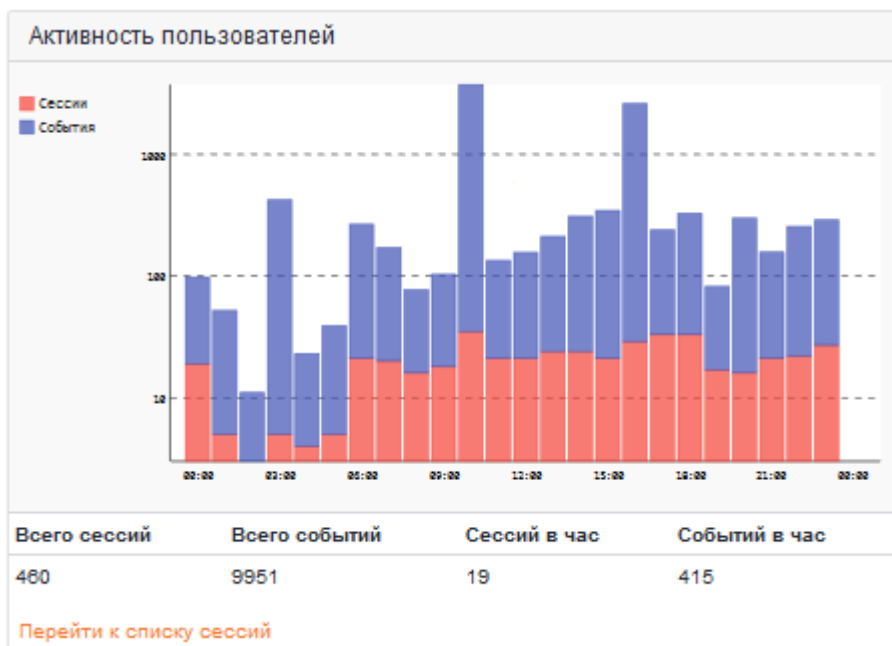
5.1 Самые продолжительные сессии

Самые продолжительные сессии			
Персона	Протокол	Сессия	Продолжительность
ploshkoav	SSH	root @ 10.126.168.96	17:07:41
ploshkoav	SSH	root @ 10.126.168.95	15:40:11
ageeys	RDP	asv @ 10.19.102.114	11:12:17
procenkosa	RDP	a.protsenko @ 172.24.253.179	10:10:32
procenkosa	RDP	a.protsenko @ 172.24.251.64	9:56:16

В данной группе представлены самые продолжительные пользовательские сессии на целевых системах за выбранный временной промежуток. Здесь указаны идентификатор сессии, персона, инициировавшая сессию, протокол соединения, а также ее продолжительность.

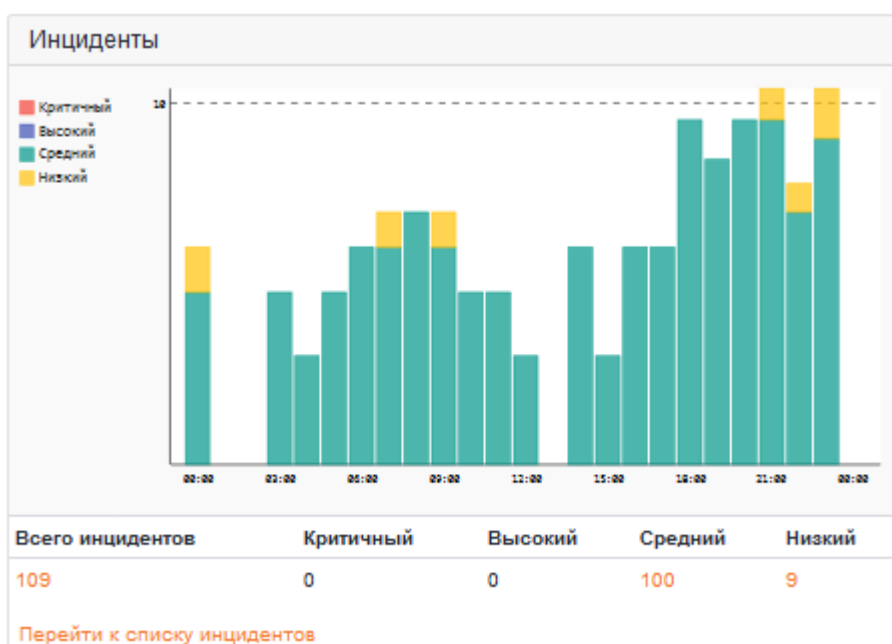
Пользователь СКДПУ НТ имеет возможность перейти в профили персон, осуществивших доступ к целевым системам (см. [раздел 7](#)), а также просмотреть данные соответствующей сессии подключения к целевой системе (см. [раздел 8](#)).

5.2 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 8](#)).

5.3 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.

5.4 Основные нарушители

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

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 7](#)).

5.5 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...			

В данной группе перечислены основные инциденты, которые за выбранный временной промежуток были инициированы персонами, их уровни критичности, а также текущий статус обработки.

Пользователь СКДПУ НТ имеет возможность перейти к полному списку инцидентов, зафиксированных за выбранный временной промежуток (см. [раздел 5.3](#)), а также перейти в профили персон, инициировавших соответствующий инцидент (см. [раздел 7](#)).

5.6 Статистика

Статистика	
Всего персон	77
Всего целевых систем	119
Всего целевых учётных записей	55
Всего загружено	626.96MB (49 файлов)
Всего скачано	3.79GB (190 файлов)
Максимум сессий в час	57

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 скаченных файлов (а также их количество) в течение пользовательских сессий, а также среднее количество пользовательских сессий в час.

5.7 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

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.

Пользователь имеет возможность перейти в профиль соответствующей персоны (см. [раздел 7](#)), к списку ее сессий (см. [раздел 8](#)), а также рассмотреть инициированные этой персоной инциденты (см. [раздел 5.3](#)).

5.8 Активные пользователи под наблюдением

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

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.

Пользователь имеет возможность перейти в профиль соответствующей персоны (см. [раздел 7](#)), к списку ее сессий (см. [раздел 8](#)), а также рассмотреть инициированные этой персоной инциденты (см. [раздел 5.3](#)).

6 ОТЧЕТЫ

6.1 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.**

6.2 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 5](#)).



Формирование отчетов производится в соответствии с правами доступа к данным, которые должны быть включены в соответствующий отчет. Таким образом, в отчет не попадают данные, доступ к которым пользователю запрещен.

Имя	Профили выполнения	Дата последнего выполнения	Действия
Top duration sessions for 3 month	8:00	2020-04-07 19:50:03	Выполнить сейчас Редактировать параметры Удалить
Sessions for 3 month	8:00	2020-05-04 19:50:04	Выполнить сейчас Редактировать параметры Удалить
Persons with Incidents this monts	8:00	2020-04-07 19:50:03	Выполнить сейчас Редактировать параметры Удалить
Top active persons with maximum targets for 30days	8:00	2020-05-04 19:50:04	Выполнить сейчас Редактировать параметры Удалить
Persons with incidents for 3 month	8:00	2020-04-07 19:50:03	Выполнить сейчас Редактировать параметры Удалить

Рисунок 5 – Раздел Отчеты > Отчеты

6.2.1 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 6.3](#)).
- Шаг 2. В появившейся форме заполнить необходимые поля (обязательные поля период или интервал дат)
- Шаг 3. Сохранить отчет нажатием [Сохранить в мои отчеты](#)

i Пользователь СКДПУ НТ имеет возможность предварительно посмотреть результаты генерирования отчета нажатием на [Просмотр](#). Отчет может быть просмотрен только в том случае, если выбрана дата или другой временной интервал, иначе будет выдано сообщение об ошибке.

- Шаг 4. Указать профиль выполнения для окончания настройки отчета. При необходимости можно указать несколько профилей.

i Для создания необходимых профилей выполнения см. [раздел 6.5.1](#).

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

При успешном создании отчета появится оповещение

Отчёт сохранён успешно x

6.2.2 Редактирование отчета

Для редактирования отчета необходимо:

- Шаг 1. В разделе **Отчеты**→**Отчеты** в строке отчета нажать [Редактировать параметры](#).
- Шаг 2. В появившейся форме изменить необходимые поля.

Шаг 3. Сохранить внесенные изменения нажатием на **Сохранить**.

При успешном сохранении отчета появится оповещение

Отчёт успешно обновлён

6.2.3 Удаление отчета

Для удаления отчета необходимо:

Шаг 1. В разделе **Отчеты**→**Отчеты** в строке отчета нажать **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

6.2.4 Генерирование отчета

Для генерирования отчета по требованию необходимо:

Шаг 1. В разделе **Отчеты**→**Отчеты** в строке отчета нажать **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 отчёт
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 возрастанию Нет		
Дата следующего выполнения:	2020-05-23 08:25:00		
2020-05-22			
Время выполнения:	Статус:	Скачивание <input checked="" type="radio"/> HTML <input type="radio"/> CSV	
08:31:10	Создан		

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 системе и характеристик сервера СКДПУ НТ.

6.3 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.

6.4 История выполнения

В рассматриваемом разделе перечислены доступные для текущего пользователя СКДПУ НТ отчеты, генерация которых происходила согласно настроенному профилю выполнения (см. [раздел 6.5](#)). Также пользователь имеет возможность скачать необходимый ему отчет в соответствующем формате (см. [раздел 6.4.1](#)).

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 6](#)).

Отчёты	Библиотека отчётов	История выполнения	Профили выполнения	Журнал авторизаций
1 2 ... 4 5 6				
2020-04-09				
Persons with Incidents this monts Время выполнения: 19:50:03		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV
Sessions for 3 month Время выполнения: 19:50:03		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV
Top duration sessions for 3 month Время выполнения: 19:50:03		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV
Persons with incidents for 3 month Время выполнения: 19:50:03		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV
2020-04-08				
Persons with Incidents this monts Время выполнения: 19:50:04		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV
Sessions for 3 month Время выполнения: 19:50:04		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV
Top duration sessions for 3 month Время выполнения: 19:50:04		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV
Persons with incidents for 3 month Время выполнения: 19:50:04		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV

Рисунок 6 – Раздел Отчеты > История выполнения

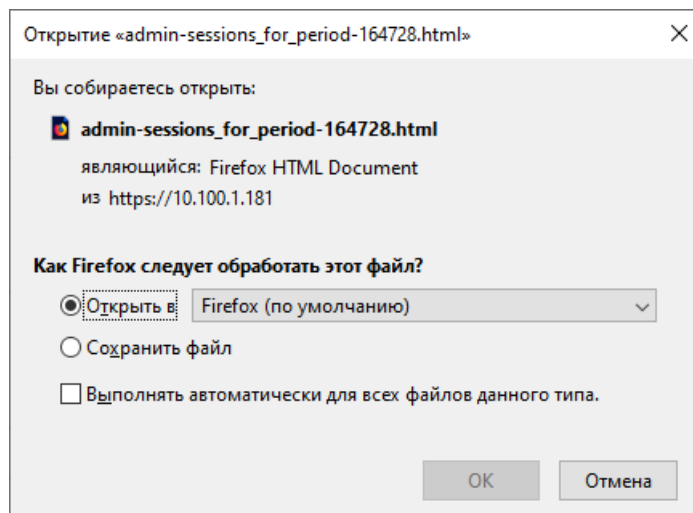
6.4.1 Скачивание отчета

Для скачивания отчета необходимо:

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

Отчёты	Библиотека отчётов	История выполнения	Профили выполнения	Журнал авторизаций
1 2 ... 4 5 6				
2020-04-09				
Persons with Incidents this monts Время выполнения: 19:50:03		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV
Sessions for 3 month Время выполнения: 19:50:03		Статус: Готов	Скачивание	<input checked="" type="radio"/> HTML <input type="radio"/> CSV

Шаг 2. Далее следовать указаниям диалогового окна



6.5 Профили выполнения

В рассматриваемом разделе представлен перечень профилей выполнения, которые доступны текущему пользователю СКДПУ НТ для редактирования и удаления (см. рисунок 7).

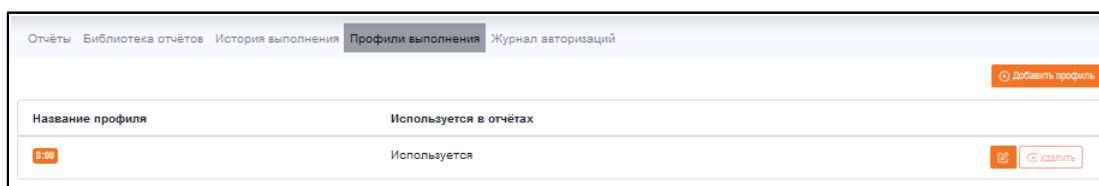


Рисунок 7 – Раздел Отчеты > Профили выполнения

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, PDF).

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.

6.5.1 Создание профиля выполнения

Для создания нового профиля выполнения необходимо:

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

Шаг 2. В появившейся форме заполнить необходимые поля

Добавить профиль выполнения

Имя (1)

Выполнять (2)
Ежедневно

Время отправки (3)

Отправлять по адресу

Отправить мне (4)

Формат (5)
 HTML
 CSV

Язык (6)
 Русский
 Английский
 Французский
 Немецкий

Сохранить

- (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.

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


Шаг 3. Сохранить профиль нажатием **Сохранить**.

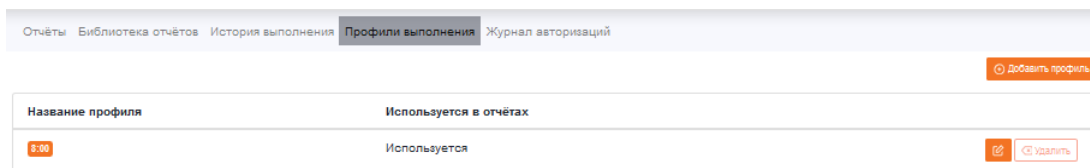
При успешном создании профиля выполнения появится оповещение

Профиль выполнения
успешно создан

6.5.2 Редактирование профиля выполнения

Для редактирования профиля выполнения необходимо:

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



Шаг 2. В появившейся форме изменить желаемые настройки


Шаг 3. Зафиксировать изменения нажатием  .

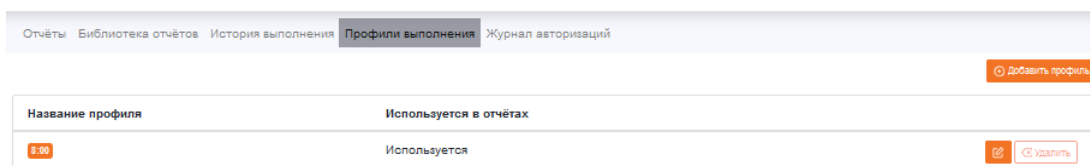
При успешном сохранении изменений параметров профиля выполнения появится оповещение

Профиль выполнения
успешно обновлён

6.5.3 Удаление профиля выполнения

Для удаления профиля выполнения необходимо:

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

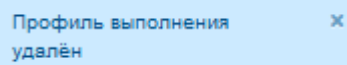


Шаг 2. Подтвердить удаление в диалоговом окне.



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

7 ПЕРСОНЫ

7.1 Общие сведения

В разделе веб-интерфейса **Персоны** СКДПУ НТ представлен перечень идентификаторов персон. Данный перечень формируется автоматически на основе списков персон, которые передаются шлюзами доступа в СКДПУ НТ. Помимо данных пользовательских сессий целевых систем в СКДПУ НТ также передается информация о персонах.

У персон может быть больше одной учетной записи (аккаунта), с помощью которых они получают доступ к целевым системам.

С каждой персоной связан индивидуальный количественный показатель – Уровень доверия (см. [раздел 7.2](#)), который рассчитывается с учетом уровня критичности инициированных этой персоной инцидентов и их количеством (см. [рисунок 8](#)).

Фото	ID	Уровень доверия	ФИО
	solovevn	350	
	krotovyuv	350	
	karhulg	384	
	krapivina	556	
	klimovnb	578	
	admin	620	
	zharovma	631	
	parma-jenkins	633	
	mds	648	
	matesheved	648	
	kovalevav	673	
	agabekovra	687	
	soln	688	
	p.garbar	690	X Y Z
	erkenovk	696	
	ris	697	
	DrimanovichNV	700	
	poluninavi	700	
	tihomirovni	700	

Рисунок 8 – Раздел Персоны

Уровень доверия формируется автоматически и не может быть изменен пользователем СКДПУ НТ.

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

С каждой персоной в СКДПУ НТ связан цифровой профиль персоны (см. [раздел 7.3](#)). 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).

7.2 Уровень доверия

За каждой персоной закреплен количественный показатель «Уровень доверия», который представляет собой профиль поведения рассматриваемой персоны, формирующийся с учетом накопленной статистики ее аномального поведения.

При генерации инцидента, источником которого является персона, значение уровня доверия уменьшается на величину, равную весу 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).

7.3 Цифровой профиль пользователя

Цифровой профиль пользователя 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 9](#)).

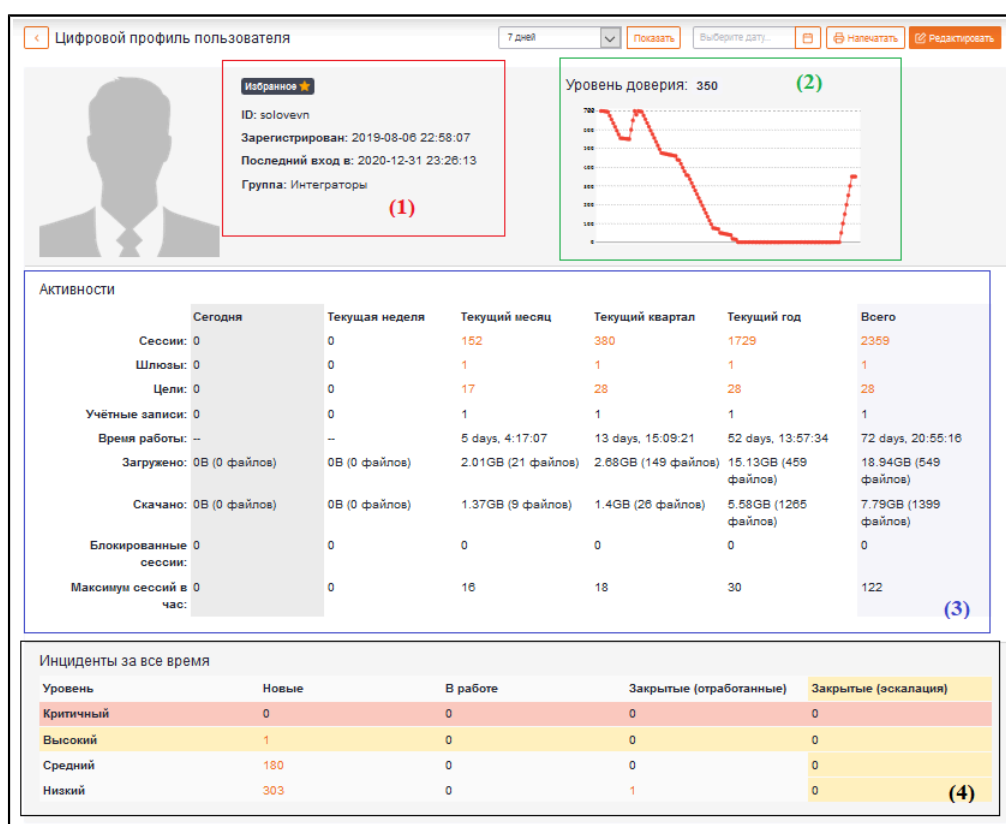


Рисунок 9 – Цифровой профиль пользователя


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

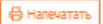
В СКДПУ НТ имеется возможность получить статистические данные за определенный временной промежуток в соответствии с выбранными значениями.

Для выбора доступны следующие временные промежутки:

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

Подтверждение осуществляется нажатием .

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

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

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

8 СЕССИИ

8.1 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.

i 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). Анализ 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 10](#) продемонстрирована форма для настройки поиска по пользовательским сессиям.

Искать текст: (1)

Ввод с клавиатуры Заголовки Файлы Процессы Буфер обмена

Включить (2) Исключить (3)

Включить цель... Включить аккаунт... Исключить цель... Исключить аккаунт...

Начиная с даты... Заканчивая датой... Начиная с даты... Заканчивая датой...

Включая персон... всех сессий

Сгруппировать (4)

дата

цель

учётная запись

персоне

Поиск выводить по 25 записей на странице

Рисунок 10 – Страница Сессии

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

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

Фрагмент результата поиска данных пользовательских сессий целевых систем без применения фильтров продемонстрирован на [рисунке 11](#).

Тип	Старт	Продолжительность	Персона / Аккаунт	Адрес клиента	Адрес цели	Шлюз	События
SSH	2020-12-31 23:59:28	0:00:00	antipov / acces-stest	10.9.130.27	10.9.130.27	DIT700	3
SSH	2020-12-31 23:59:27	0:00:00	konchaeva / konchaeva	172.18.24.29	172.17.16.97	DIT700	3
SSH	2020-12-31 23:58:28	0:00:00	antipov / acces-stest	10.9.130.27	10.9.130.27	DIT700	3
SSH	2020-12-31 23:58:26	0:00:01	konchaeva / konchaeva	172.18.24.29	172.17.16.97	DIT700	3
SSH	2020-12-31 23:57:28	0:00:00	antipov / acces-stest	10.9.130.27	10.9.130.27	DIT700	3
SSH	2020-12-31 23:57:26	0:00:01	konchaeva / konchaeva	172.18.24.29	172.17.16.97	DIT700	3
SSH	2020-12-31 23:56:48	0:00:01	antipov / acces-stest	10.9.130.27	10.9.130.27	DIT700	3

(1) (2) (3) (4) (5) (6) (7) (8)

Рисунок 11 – 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.

При нажатии на кнопку **Добавить фильтры** 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 **Напечатать**.

8.2 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 11](#)) выбрать интересующую сессию.

Пример профиля пользовательской сессии представлен на [рисунке 12](#). 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.

The screenshot shows a user session card with the following details:

- ID: 187a453f821448b6005056b04f93
- Тип: SSH
- Персона: kulicyna
- Адрес клиента: 172.18.18.74
- Старт: 21-04-2023 17:59:41
- Окончание: 21-04-2023 18:00:15
- Продолжительность: 0:00:34
- Цель: root @ SPPR-FILE-TEST-10.89.72.1 (10.89.72.1)
- Шлюз: skdpu-02p
- Видео: 800x600 @ 25fps MPEG4
- Инциденты: 1

Below the details is a timeline chart showing the session duration from 17:59:40 to 18:00:15. The chart includes a legend with categories: СОБЫТИЕ Низкая Плотность (green), Низкий (yellow), СЕССИЯ (blue), and отметки инцидентов (yellow dot). A red circle (1) is placed next to the session details, and another red circle (2) is placed below the chart.

Дата и время записи	Тип события	Данные
21-04-2023 17:59:41	SESSION_ESTABLISHED_SUCCESSFULLY	
21-04-2023 17:59:47	KBD_INPUT	ssh akunitsyn@10.89.72.40
21-04-2023 17:59:49	KBD_INPUT	yes
21-04-2023 18:00:15	KBD_INPUT	rootsu

Рисунок 12 – Карточка пользовательской сессии

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

Пользователь СКДПУ НТ имеет возможность, при наличии достаточных оснований, создать инцидент, подробнее (см. [раздел 9.3](#)).

9 ИНЦИДЕНТЫ

9.1 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 9.3](#)).

Расследование инцидентов начинается с назначения ответственного лица (см. [раздел 9.5](#)), 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 9.4](#)).

По результатам расследования инцидента происходит его закрытие с указанием причины возникновения (см. [раздел 9.6](#)).

Действия некоторых персон могут инициировать инциденты, которые таковыми не являются. СКДПУ НТ предоставляет возможность указать детекторы аномалий, которые не будут применяться к событиям, которые инициируются определенными персонами (см.).

Все действия в течение всего времени обработки инцидента фиксируются в соответствующем виде (см. [раздел 9.2](#)).

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 с помощью списков ограничения доступа к данным (подробнее см. Руководство администратора).

Пользователь СКДПУ НТ имеет возможность осуществлять поиск инцидентов, предварительно настроив следующие фильтры (см. [рисунок 13](#)):

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

Рисунок 13 – Раздел Инциденты



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

Ниже представлен фрагмент результата поиска инцидентов без применения фильтров (см. рисунок 14).

ID (1)	Дата регистрации (2)	Источник (3)	Процессор (4)	Уровень (5)	Статус (6)	Причина (7)	Назначен (8)	Уведомления (9)
NA-1087017	2020-05-22 19:38:27	admin	Новый доступ	Низкий	Новые			
KPE-1087019	2020-05-22 17:09:32	admin	Разрыв сессии	Низкий	Новые			
KPE-1087018	2020-05-22 17:09:31	admin	Разрыв сессии	Низкий	Новые			
NA-1087016	2020-05-22 16:37:52	admin	Новый доступ	Низкий	Новые			
NA-1087020	2020-05-22 16:17:12	admin	Новый доступ	Низкий	Новые			
TF-1087015	2020-05-21 13:02:56	mds	Необычное время работы	Низкий	Новые			
SA-1087014	2020-05-21 10:05:52	soln	Source address	Низкий	Новые			
TF-1087013	2020-05-21 00:01:21	mds	Необычное время работы	Низкий	Новые			
PD-1087012	2020-05-20 21:41:19	mds	Permission denied	Низкий	Новые			
NA-1087011	2020-05-20 21:41:01	mds	Новый доступ	Низкий	Новые			
TF-1087010	2020-05-20 21:06:35	mds	Необычное время работы	Низкий	Новые			
NA-1087009	2020-05-20 20:41:32	rls	Новый доступ	Низкий	Новые			
TF-1087008	2020-05-20 20:41:29	mds	Необычное время работы	Низкий	Новые			
NA-1087007	2020-05-20 20:41:29	mds	Новый доступ	Низкий	Новые			

Рисунок 14 – 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) – тип инцидента.
- (5) – уровень критичности инцидента.
- (6) – текущий статус инцидента.

- (7) – причина возникновения инцидента.
- (8) – назначенный ответственный за обработку инцидента.
- (9) – 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 **Напечатать**.

9.2 Профиль инцидента

Профиль инцидента содержит подробный перечень данных о выбранном инциденте. Для перехода к профилю инцидента необходимо из перечня инцидентов (см. [рисунок 14](#)) выбрать интересующий инцидент.

Пример профиля инцидента представлен на [рисунок 15](#). В профиле 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 профиля инцидента пользователь СКДПУ НТ имеет возможность просмотреть цифровой профиль персоны (см. [раздел 7.3](#)), действия которой явились возможной причиной возникновения рассматриваемого инцидента, а также перейти к сессии (см. [раздел 8.2](#)), во время которой произошел инцидент.

Инциденты NA-1087017

Называть мне Называть Закрывать (отработано) Закрывать (ложное срабатывание) Напечатать Редактировать

ID NA-1087017 (1)

Дата регистрации 2020-05-22 16:38:27

Персона admin

Сессия 1723bbf44e8e696b000c29eee193

Тип Новый доступ

Уровень Низкий

Статус Новые

Назначен Нет владельца

Данные new target_ip: 10.100.64.2

Подробности: (2)

Дата и время записи	Тип события	Данные
2020-05-22 16:38:27	SESSION_ESTABLISHED_SUCCESSFULLY	

История: (3)

Отметка времени	Отредактировано	Изменения	Комментарий
-----------------	-----------------	-----------	-------------

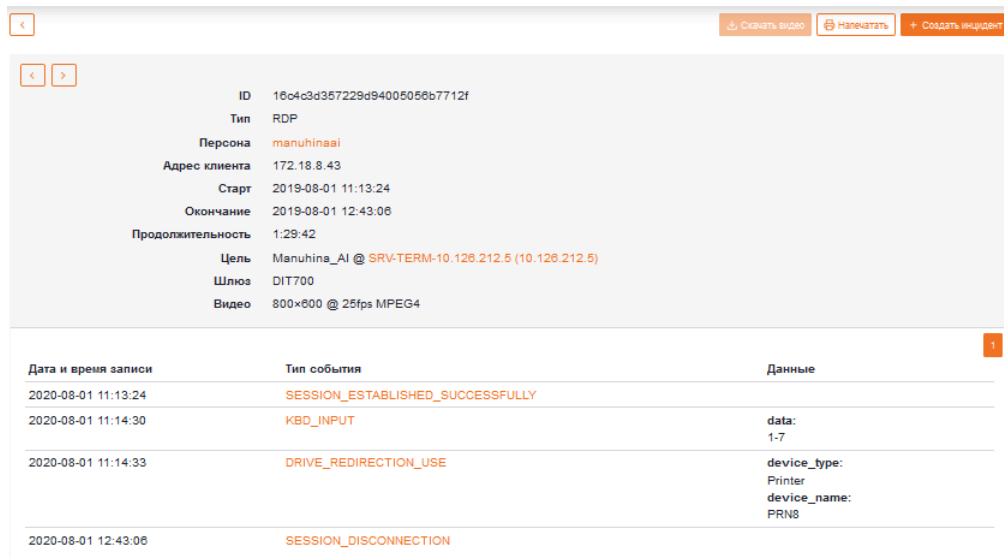
Рисунок 15 – Карточка инцидента

Пользователь может распечатать профиль инцидента, нажав **Напечатать**.

9.3 Создать инцидент

Для создания инцидента необходимо:

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



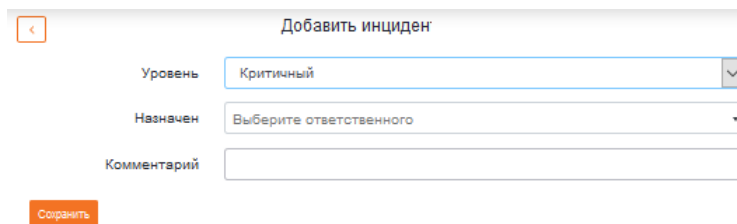
The screenshot shows a user session profile with the following details:

- ID: 16c4c3d357228d94005056b7712f
- Тип: RDP
- Персона: manuhinaai
- Адрес клиента: 172.18.8.43
- Старт: 2019-08-01 11:13:24
- Окончание: 2019-08-01 12:43:06
- Продолжительность: 1:29:42
- Цель: Manuhina_AI @ SRV-TERM-10.126.212.5 (10.126.212.5)
- Шлюз: DIT700
- Видео: 800x600 @ 25fps MPEG4

Below the details is a table of events:

Дата и время записи	Тип события	Данные
2020-08-01 11:13:24	SESSION_ESTABLISHED_SUCCESSFULLY	
2020-08-01 11:14:30	KBD_INPUT	data: 1-7
2020-08-01 11:14:33	DRIVE_REDIRECTION_USE	device_type: Printer device_name: PRN8
2020-08-01 12:43:06	SESSION_DISCONNECTION	

Шаг 2. В появившейся форме заполнить необходимые поля



The screenshot shows a form titled "Добавить инцидент" with the following fields:

- Уровень: Критичный (dropdown menu)
- Назначен: Выберите ответственного (dropdown menu)
- Комментарий: (text input field)

A "Сохранить" button is located at the bottom left of the form.

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

При успешном создании инцидента появится оповещение

Инцидент успешно создан ✕

9.4 Редактировать инцидент

Для редактирования параметров инцидента необходимо:

Шаг 1. В профиле инцидента нажать [Редактировать](#) .

The screenshot shows the user interface for an incident profile. At the top, there is a header bar with the title "Инциденты CLM-1002823" and several action buttons: "Для внесения в белый список", "Назначить мне", "Назначить...", and "Закрыть (отработано)". Below the header, there are three more buttons: "Закрыть (ложное срабатывание)", "Напечатать", and "Редактировать". The main content area displays the incident details in a list format:

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 изменить необходимые поля

Инциденты MAN-1087021

ID: MAN-1087021
Дата регистрации: 2020-05-24 00:58:05
Персона: manuhinasi
Сессия: 16c4c3d357229d94005056b7712f
Тип: Создан вручную

Уровень
Низкий

Статус
Новые

Причина
Отсутствует

Комментарий

Назначен
Выберите ответственного

Комментарий для истории

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.
- (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 **Сохранить**.

При успешном редактировании инцидента появится оповещение

Данные инцидента
обновлены

9.5 Назначить ответственного за обработку инцидента

Для назначения ответственного за обработку инцидента необходимо:

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

Инциденты CLM-1002823

Для внесения в белый список Назначить мне Назначить ... Закреть (отработано)

Закреть (ложное срабатывание) Напечатать Редактировать

ID	CLM-1002823
Дата регистрации	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	192.168.3.100
Данные	gray: *ls -la.*

Шаг 2. В появившейся форме (см. [раздел 9.4](#)) выбрать ответственного лицо в поле **Назначен**

Назначен

Выберите ответственного



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

Выберите ответственного

Закреть Сохранить

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

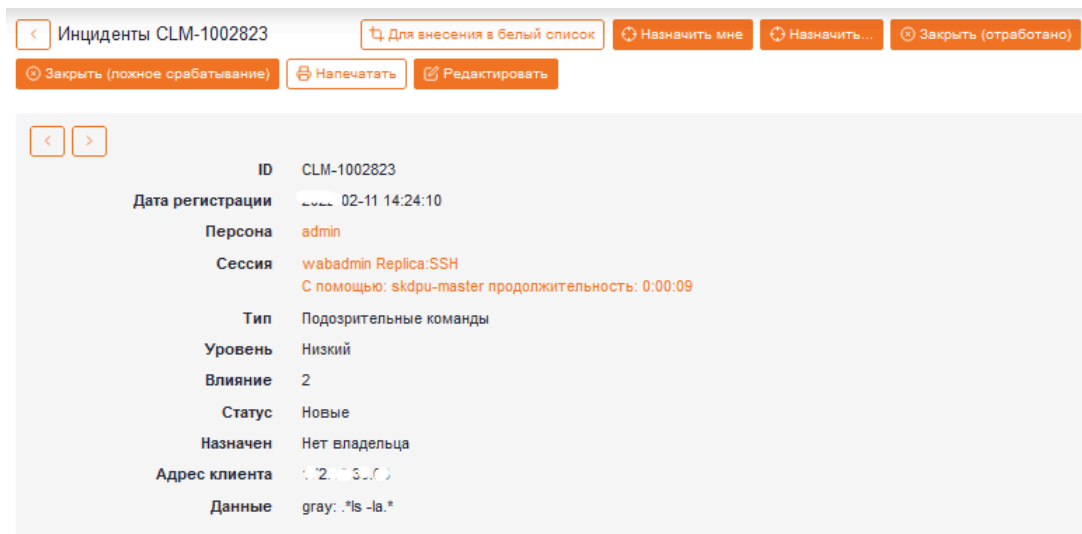
При успешном редактировании инцидента появится оповещение

Данные инцидента
обновлены

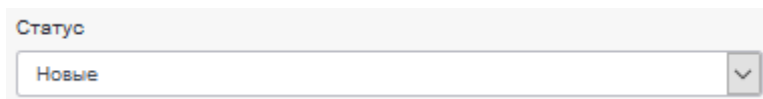
9.6 Закрывать инцидент

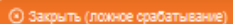
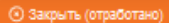
Для закрытия инцидента необходимо:

Шаг 1. В профиле инцидента нажать  .

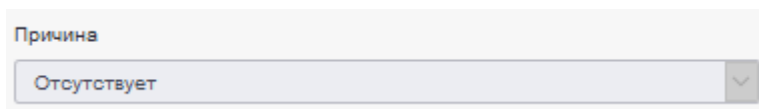


Шаг 2. В появившейся форме (см. [раздел 9.4](#)) выбрать статус инцидента **Закрывать** в поле **Статус**




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

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



Шаг 4. Сохранить инцидент нажатием на  .

При успешном редактировании инцидента появится оповещение

Данные инцидента обновлены 

10 КОМПОНЕНТЫ

10.1 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;

10.2 Шлюзы

В данном разделе перечислены шлюзы доступа, с которых есть зарегистрированные сессии в системе и данные пользовательских сессий целевых систем (см. [рисунок 16](#)).

ID (1)	Адрес (2)	Версия ПО (3)	Время последнего использования (4)	Статус (5)
skdpu-node	https://10.100.68.17	7.0 (API v2.4)	...-03 09:46:19	OK
skdpu-master	https://10.100.68.16	7.0 (API v2.4)	...-02 13:43:03	OK
skdpu-01p		(API)	... 25 00:10:14	данные не введены
skdpu-02p		(API)	...-15 00:03:18	данные не введены
skdpu-03p		(API)	... 15 00:02:25	данные не введены

Рисунок 16 – Раздел Компоненты > Шлюзы

i 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.

i Возможны следующие состояния:

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

При нажатии на кнопку **Добавить фильтры** появляется дополнительное поле, в котором можно выбрать тип (1)-(5), где будет задана дополнительная маска для более удобного поиска.

Для перехода в карточку шлюза необходимо нажать на нужную строку, после чего появится более детальная информация (см. **рисунок 17**).

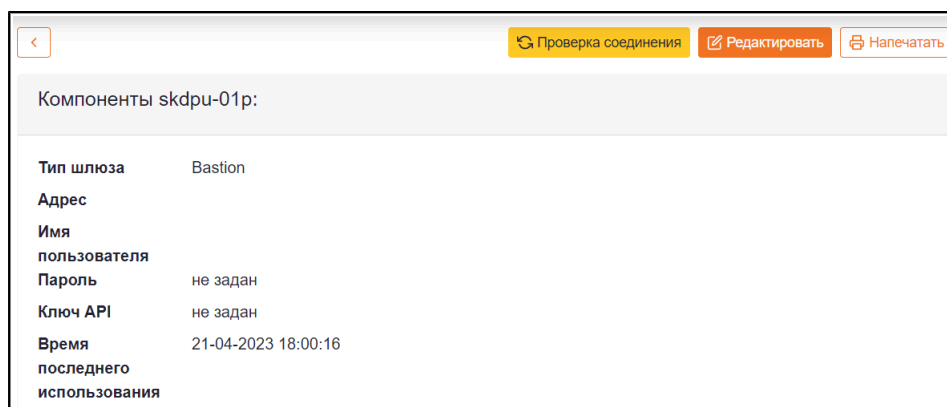


Рисунок 17 – Карточка шлюза

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

Проверка соединения, или напечатать, нажав на кнопку **Напечатать**.

Для редактирования шлюза необходимо нажать на кнопку **Редактировать**.

Шаг 1. На странице редактирования необходимо заполнить обязательные поля **Адрес** и **Имя пользователя**. Поля **Пароль** и **Ключ API** имеют поля подтверждения.



При этом, если эти данные не ввести, то в карточке шлюза будет выведено соответствующее предупреждение.

Шаг 2. Для сохранения введенных данных необходимо нажать на кнопку **Сохранить**.

При успешном сохранении будет выведено сообщение:

Данные шлюза обновлены ✕

10.3 Цели

В рассматриваемом разделе перечислены целевые устройства, к которым осуществляли доступ персоны через соответствующий шлюз доступа (см. [рисунок 18](#)).

(1) Имя устройства	(2) IP-адрес цели	(3) ☆ Тип	(4) Время последнего использования
Replica	10.10.10.10	☆ SSH	13-03 09:46:19
Server2019	10.10.10.3	☆ RDP	13-03-02 14:38:45
CentOS	10.10.10.10	☆ SSH	02-22 17:25:25
KADRY-APP114T-1T	10.2.1.1	☆ RDP	01-25 00:10:14
MJK-APP1T-1.1	10.10.10.7	☆ SSH	01-25 00:09:05

Рисунок 18 – Раздел Компоненты > Цели

- (1) – имя устройства;
- (2) – IP-адрес цели;
- (3) – тип подключения;
- (4) – время и дата последнего использования.

При нажатии на кнопку **Добавить фильтры** появляется дополнительное поле, в котором можно выбрать тип (1)-(4), 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 **Напечатать**.

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 19](#)).

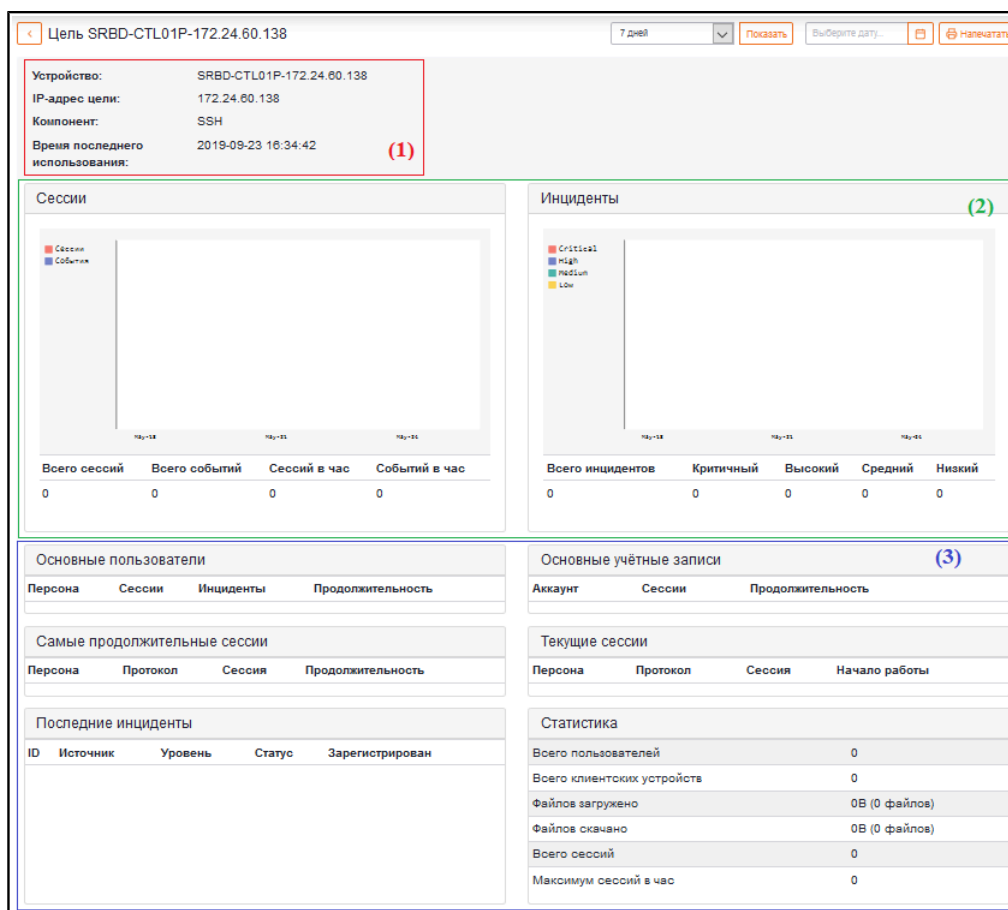


Рисунок 19 – Статистика устройства

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 [Показать](#).

Также пользователь имеет возможность выбрать для просмотра конкретную дату, подтвердив нажатием [📅](#).

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

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.
HTTP	HyperText Transfer Protocol — протокол передачи гипертекста.
LAN	Local Area Network — локальная компьютерная сеть.
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к каталогам) — протокол прикладного уровня для доступа к службе каталогов X.500
RLOGIN	Remote LOGIN — удалённый вход в систему.
SATA	Serial Advanced Technology Attachment — последовательный интерфейс обмена данными с накопителями информации.
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.
SCSI	Small Computer System Interface — набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами.
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
URL	Uniform Resource Locator (унифицированный указатель ресурса) — система унифицированных адресов электронных ресурсов.

АРМ Автоматизированное рабочее место

ПО Программное обеспечение

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 – Форма ввода логина и пароля.....	8
Рисунок 2 – Ошибка входа.....	9
Рисунок 3 – Интерфейс СКДПУ НТ.....	10
Рисунок 4 – Раздел Мониторинг.....	12
Рисунок 5 – Раздел Отчеты Отчеты.....	19
Рисунок 6 – Раздел Отчеты История выполнения.....	22
Рисунок 7 – Раздел Отчеты Профили выполнения.....	23
Рисунок 8 – Раздел Персоны.....	27
Рисунок 9 – Цифровой профиль пользователя.....	28
Рисунок 10 – Страница Сессии.....	30
Рисунок 11 – Пример выборки сессий.....	31
Рисунок 12 – Карточка пользовательской сессии.....	32
Рисунок 13 – Раздел Инциденты.....	34
Рисунок 14 – Пример представления результатов выборки всех инцидентов.....	34
Рисунок 15 – Карточка инцидента.....	35
Рисунок 16 – Раздел Компоненты Шлюзы.....	41
Рисунок 17 – Карточка шлюза.....	42
Рисунок 18 – Раздел Компоненты Цели.....	43
Рисунок 19 – Статистика устройства.....	44

ПЕРЕЧЕНЬ ТАБЛИЦ

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

