



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

Руководство администратора

RU.33654484.0001-01 91 01

Листов 113

АННОТАЦИЯ

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

Настоящий документ содержит сведения о назначении и условиях применения СКДПУ НТ, общее описание процесса администрирования СКДПУ НТ.

Настоящий документ содержит подробное описание действий по конфигурированию, сопровождению и администрированию СКДПУ НТ в целях обеспечения максимальной безопасности эксплуатации.

СОДЕРЖАНИЕ

1 Назначение и область применения СКДПУ НТ.....	6
2 Условия функционирования.....	7
2.1 Общие сведения.....	7
2.2 Описание установки СКДПУ НТ.....	7
2.3 Структура директорий СКДПУ НТ.....	7
2.4 Требования к администратору СКДПУ НТ.....	8
2.5 Контроль целостности дистрибутива СКДПУ НТ.....	8
2.6 Контроль целостности исполняемых файлов СКДПУ НТ.....	8
2.7 Минимальные характеристики аппаратно-программного обеспечения АРМ.....	9
3 Описание интерфейсов.....	10
3.1 Консоль администрирования.....	10
3.1.1 Вход.....	10
3.1.2 Использование консоли администрирования.....	10
3.2 Графический веб-интерфейс.....	10
3.2.1 Вход.....	10
3.2.2 Описание интерфейса.....	12
4 Настройка прав доступа.....	15
4.1 Общие сведения.....	15
4.2 Пользователи СКДПУ НТ.....	15
4.2.1 Добавление учетной записи пользователя СКДПУ НТ.....	16
4.2.2 Удаление учетной записи пользователя СКДПУ НТ.....	18
4.2.3 Редактирование данных учетной записи пользователя СКДПУ НТ.....	18
4.2.4 Доменный пользователь СКДПУ НТ.....	21
4.3 Роли СКДПУ НТ.....	21
4.3.1 Добавление новой роли.....	28
4.3.2 Редактирование разрешений для существующей роли.....	29
4.3.3 Удаление существующей роли.....	30
4.4 Управление доступом к данным.....	30
4.4.1 Создание ограничения доступа к данным.....	31
4.4.2 Редактирование ограничения доступа к данным.....	33
4.4.3 Формирование списков ограничения доступа к данным.....	33
4.4.4 Удаление ограничения доступа к данным.....	36
4.5 Управление парольной политикой пользователей СКДПУ НТ.....	37
4.6 Группы LDAP.....	37
5 Детекторы аномалий.....	40
5.1 Общие сведения.....	40

5.2 Детектирование потенциально опасных команд.....	42
5.3 Детектирование принудительного блокирования сессий.....	43
5.4 Контроль привычного времени работы.....	43
5.5 Контроль изменения уровня доверия.....	44
5.6 Контроль стандартных команд.....	46
5.7 Контроль привычных сетевых адресов.....	47
5.8 Контроль эффективности работы.....	48
5.9 Индикаторы взрывной активности.....	48
5.10 Детектор новых доступов.....	49
5.11 Детектор проблем с правами доступа к файлам.....	50
5.12 Детектор туннелей и прыжков.....	51
5.13 Детектор входов помимо бастиона.....	52
5.14 Анализатор ошибок авторизации.....	52
5.15 Детектор забытых персон.....	53
5.16 Количество переданных файлов.....	54
5.17 Детектор сканеров.....	55
6 Настройка источников пользовательских сессий целевых систем.....	57
6.1 Шлюз доступа.....	57
6.2 Файл с событиями.....	58
6.3 Системы сторонних производителей.....	59
7 Настройка.....	64
7.1 Общие сведения.....	64
7.2 Основные настройки.....	64
7.2.1 Настройка параметров соединения с почтовым сервером.....	64
7.2.2 Настройка веб-интерфейса.....	65
7.2.3 Управление системой отчетов.....	66
7.3 Системные настройки.....	67
7.4 Настройки LDAP.....	68
7.4.1 Домен LDAP.....	69
7.4.2 Сервер LDAP.....	72
7.4.3 Группы LDAP.....	73
7.5 Конфигурация журналирования.....	76
7.5.1 Добавить подключение к удаленному серверу.....	77
7.5.2 Удалить подключение к удаленному серверу.....	77
7.5.3 Активировать/деактивировать подключение к удаленному серверу.....	78
7.6 Информация о лицензии.....	78
8 Целевые системы.....	79
8.1 Общие сведения.....	79

8.2 Настройка аутентификации шлюзов.....	79
9 Аудит безопасности.....	81
9.1 Общие сведения.....	81
9.2 Журнал авторизаций.....	82
10 Сценарии использования.....	84
10.1 Добавление LDAP-домена.....	84
10.2 Добавление LDAP-сервера.....	84
10.3 Добавления роли.....	85
10.4 Связывание роли и доменной группы.....	85
11 Обслуживание СКДПУ НТ.....	86
11.1 Диагностика СКДПУ НТ и его сервисов.....	86
11.2 Диагностика СКДПУ НТ через консоль ОС.....	87
11.3 Сброс пароля администратора веб-интерфейса СКДПУ НТ.....	88
11.4 Смена паролей учетных записей консоли администрирования.....	88
11.5 Добавление файла лицензии.....	88
11.6 Резервное копирование и восстановление параметров.....	89
11.6.1 Создание резервных копий.....	89
11.6.2 Восстановление из резервных копий.....	90
11.7 Удаление устаревших данных пользовательских сессий целевых систем.....	90
11.8 Обновление СКДПУ НТ.....	90
11.9 Обращение в службу поддержки.....	91
12 Возможные вопросы.....	93
12.1 Нарушение целостности компонентов СКДПУ НТ.....	93
12.2 Недостаток свободного места в хранилище.....	93
12.3 Отсутствие файла лицензии.....	94
Приложение А. Перечень утилит консоли администрирования СКДПУ НТ.....	95
Перечень сокращений.....	108
Перечень рисунков.....	111
Перечень таблиц.....	112
История изменений.....	113

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 УСЛОВИЯ ФУНКЦИОНИРОВАНИЯ

2.1 Общие сведения

СКДПУ НТ представляет собой серверное приложение, функционирующее на UNIX-платформе, реализованной в виде сервера под управлением ОС Astra Linux 1.6SE. Пользовательский интерфейс СКДПУ НТ реализован в форме веб-интерфейса, доступного через браузер.

Браузер должен быть установлен перед началом работы с СКДПУ НТ. Для корректной работы СКДПУ НТ рекомендуется в настройках браузера разрешить выполнение javascript и сохранение файлов cookies.

СКДПУ НТ имеет информационное сопряжение с веб-сервером HTTP Apache и СУБД PostgreSQL для обеспечения передачи и хранения данных.

2.2 Описание установки СКДПУ НТ

Установка и первоначальная настройка СКДПУ НТ производится в соответствии с Руководством по установке.

2.3 Структура директорий СКДПУ НТ

СКДПУ НТ имеют следующую структуру директорий:

- /opt/skdpu-nt/ – корневая директория СКДПУ НТ;
- /opt/skdpu-nt/bin/ – директория, содержащая утилиты администрирования;
- /opt/skdpu-nt/var/ – директория, где располагаются файлы базы данных, полнотекстового индекса СКДПУ НТ;
- /opt/skdpu-nt-data/ – директория, где располагаются журналы СКДПУ НТ, сгенерированные отчеты, а также данные пользовательских сессий целевых систем в виде отдельных файлов;
- /opt/skdpu-nt-data/log/ – директория, где располагаются файлы журналов СКДПУ НТ.
- /opt/skdpu-nt-data/log/cef.log содержит сообщения о событиях в рамках пользовательских сессий целевых систем, а также о событиях в рамках доступа к веб-интерфейсу СКДПУ НТ.
- /opt/skdpu-nt-data/log/error.log содержит сообщения об ошибках от сервисов СКДПУ НТ.
- /opt/skdpu-nt-data/log/reject.log – события, которые обработались системой как неизвестные для анализа.

2.4 Требования к администратору СКДПУ НТ

Администратор СКДПУ НТ должен иметь высшее профильное образование. В обязанности администратора СКДПУ НТ входит:

- настройка СКДПУ НТ в соответствии с предъявляемыми требованиями безопасности;
- обеспечение безопасности СКДПУ НТ и его компонентов в течение всего времени эксплуатации;
- при эксплуатации СКДПУ НТ неукоснительно следовать инструкциям, указанным в настоящем документе.

2.5 Контроль целостности дистрибутива СКДПУ НТ

i Перед проведением контроля целостности файлов дистрибутива СКДПУ НТ необходимо убедиться в наличии файла проекта `skdpu_nt.prj`, который должен быть создан на этапе развертывания СКДПУ НТ.

Необходимо выполнить следующие шаги:

Шаг 1. Вставить носитель с дистрибутивом СКДПУ НТ в дисковод.

Шаг 2. Получить права суперпользователя.

Шаг 3. Осуществить контроль целостности файлов дистрибутива СКДПУ НТ

```
ufix -y /home/ntadmin/skdpu_nt.prj
```

При нарушении целостности набора файлов, указанных в файле проекта, генерируется соответствующее оповещение.

Шаг 4. Сгенерировать отчет в формате `html`

```
ufix -h /home/ntadmin/skdpu_nt.prj /home/ntadmin/  
skdpu_nt_data.html
```

Итоговая контрольная сумма заносится в таблицу 6 Формуляра.

2.6 Контроль целостности исполняемых файлов СКДПУ НТ

i Перед проведением контроля целостности исполняемых файлов СКДПУ НТ необходимо убедиться в наличии файла проекта `skdpu_nt_inst.prj`, который должен быть создан на этапе развертывания СКДПУ НТ.

Необходимо выполнить следующие шаги:

Шаг 1. Получить права суперпользователя.

Шаг 2. Осуществить контроль целостности исполняемых файлов СКДПУ НТ

```
ufix -y /home/ntadmin/skdpu_nt_inst.prj
```

При нарушении целостности набора файлов, указанных в файле проекта, генерируется соответствующее оповещение.

Шаг 3. Сгенерировать отчет в формате html

```
ufix -h /home/ntadmin/skdpu_nt_inst.prj /home/ntadmin/skdpu_nt_inst_дата.html
```

Итоговая контрольная сумма заносится в таблицу 6 Формуляра.

2.7 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»

3 ОПИСАНИЕ ИНТЕРФЕЙСОВ

3.1 Консоль администрирования

Учетная запись `ntadmin` это учетная запись с низкими правами, которой разрешен вход в консоль и вход по протоколу SSH на сервер СКДПУ НТ.

Учетная запись `ntsuper` является более привилегированной, и для данной учетной записи разрешено повышение прав до суперпользователя, выполнив команду `sudo -i`.

3.1.1 Вход

Для получения доступа к консоли администрирования СКДПУ НТ необходимо:

Шаг 1. В консоли ОС сервера, где установлен СКДПУ НТ, осуществить вход с паролем учетной записи `ntadmin`.

Шаг 2. Выполнить команду `super` с вводом пароля учетной записи `ntsuper`.

Шаг 3. Выполнить команду `sudo -i` с вводом пароля учетной записи `ntsuper`.

При успешной авторизации на всех шагах администратор получает доступ к консоли администрирования с правами суперпользователя.

3.1.2 Использование консоли администрирования

Консоль администрирования СКДПУ НТ предназначена для настройки и последующего обслуживания СКДПУ НТ и его компонентов.

Типичные сценарии обслуживания СКДПУ НТ представлены в [разделе 11](#).

Перечень утилит консоли администрирования представлен в [приложении А](#).



Для использования утилит консоли администрирования необходимы права суперпользователя.

3.2 Графический веб-интерфейс

3.2.1 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)

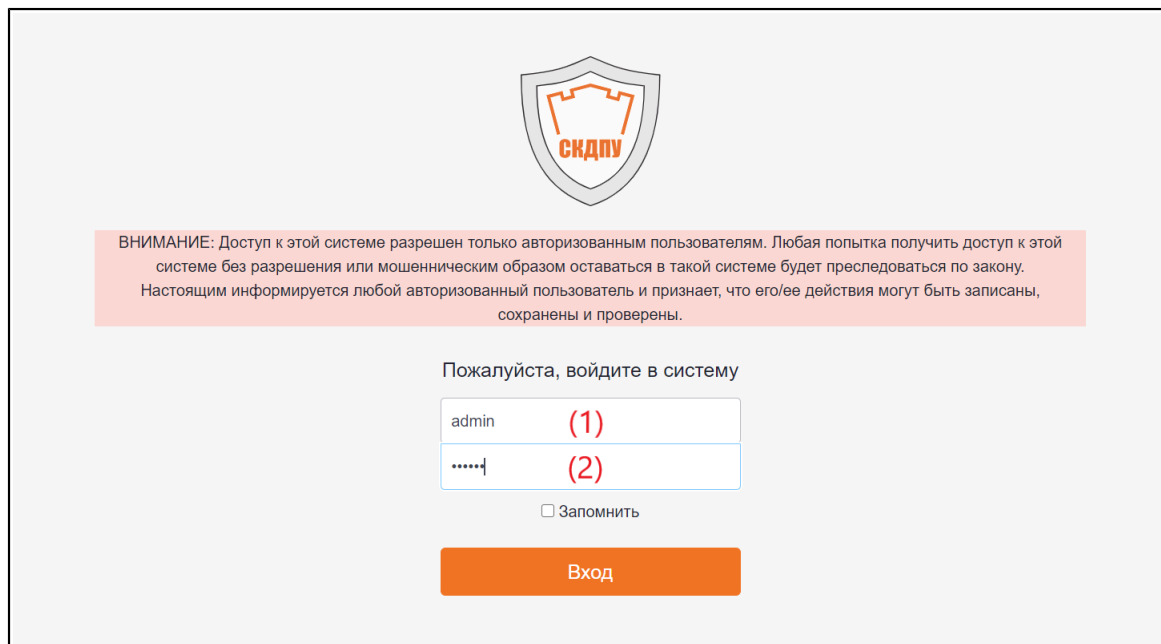


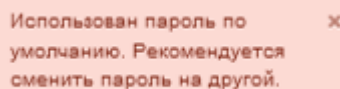
Рисунок 1 – Форма ввода логина и пароля

Шаг 3. Нажать на кнопку  .

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



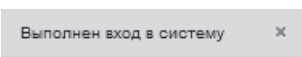
При первом входе, после установки СКДПУ НТ, администратор должен ввести следующую пару (логин, пароль): (`admin`, `admin`). Рекомендуется сразу после авторизации сменить пароль для соблюдения требований безопасности (см. [раздел 4.2.3.1](#)). Если администратор будет использоваться пароль по умолчанию, то при каждом входе в веб-интерфейс СКДПУ НТ будет выводиться следующее сообщение



Использован пароль по умолчанию. Рекомендуется сменить пароль на другой.

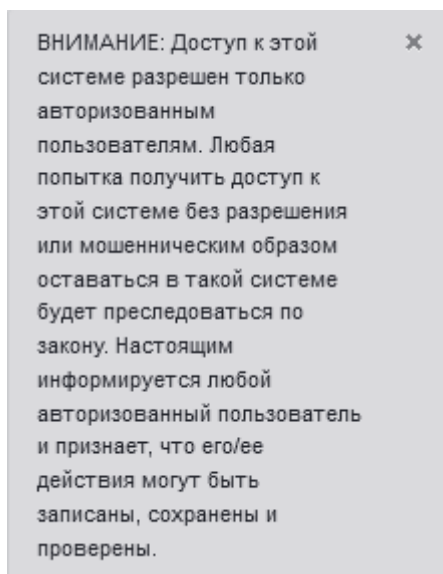
При успешной авторизации в правом нижнем углу появится следующая информация:

- выполнен вход в систему

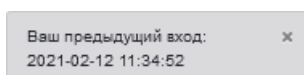


Выполнен вход в систему

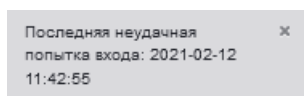
- предупреждение пользователя об ответственности неправомерного использования и мерах защиты, реализованных в СКДПУ НТ



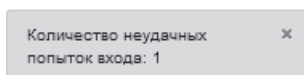
- дата и время предыдущей успешной авторизации



- 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

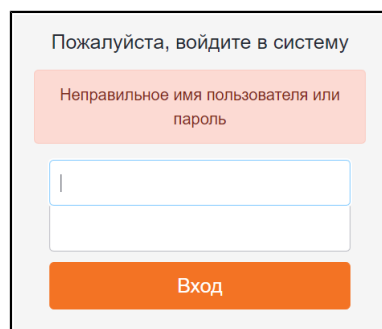


Рисунок 2 – Ошибка входа

3.2.2 Описание интерфейса

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

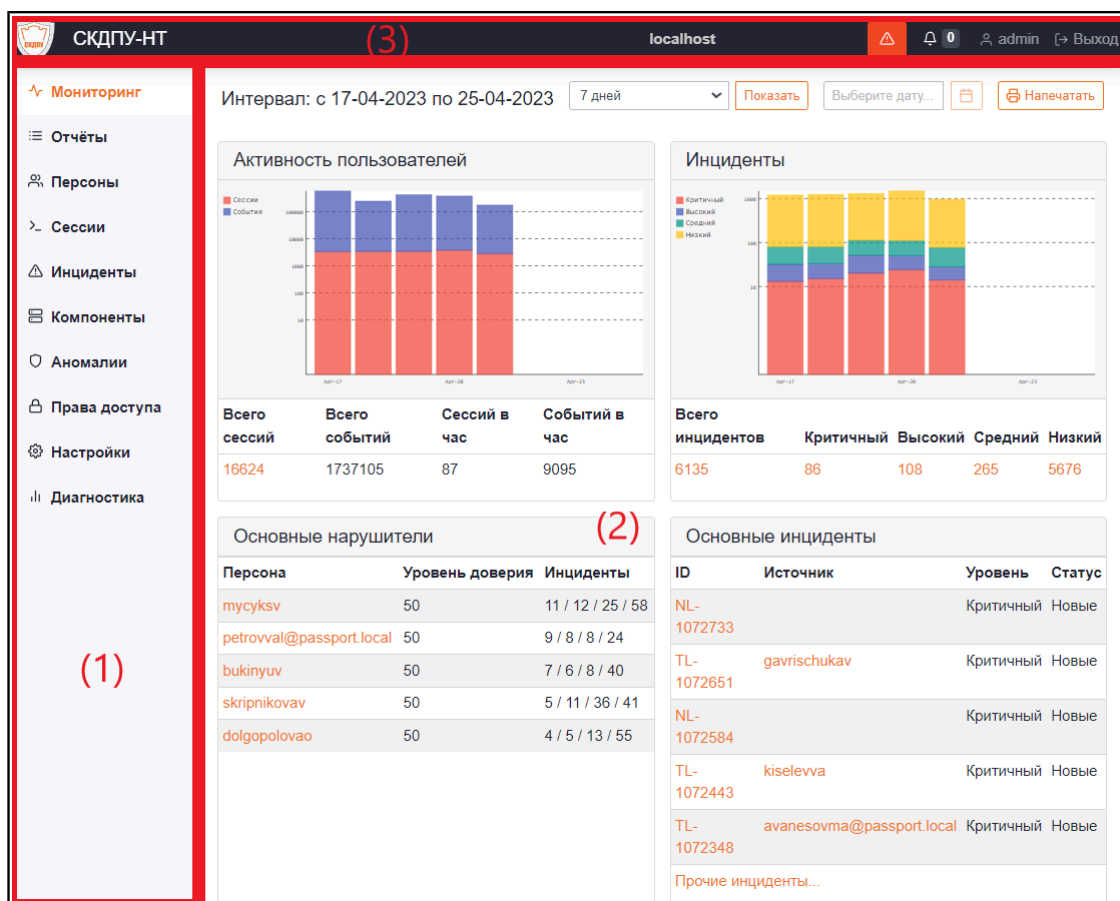


Рисунок 3 – Интерфейс СКДПУ НТ

- (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 веб-интерфейса **Мониторинг**;
- (2) – оповещение о существующих событиях в функционировании СКДПУ НТ (см. раздел 12). При нажатии происходит переход в раздел **Диагностика**;
- (3) – оповещение о количестве зафиксированных за последнее время инцидентах в пользовательских сессиях целевых систем. При нажатии происходит переход в раздел **Инциденты**;
- (4) – идентификатор текущего пользователя СКДПУ НТ. При нажатии происходит переход в учетную запись пользователя СКДПУ НТ, где можно редактировать его данные и настройки (см. раздел 4.2.3);
- (5) – кнопка выхода. При нажатии происходит окончание сессии текущего пользователя СКДПУ НТ.



Администратор СКДПУ НТ имеет максимальные привилегии, и ему разрешен доступ ко всем разделам.

4 НАСТРОЙКА ПРАВ ДОСТУПА

4.1 Общие сведения

При настройке прав доступа пользователей к функциональным возможностям СКДПУ НТ необходимо руководствоваться нормативной документацией по обеспечению информационной безопасности, принятой в эксплуатирующей организации, например, «Политика безопасности организации».

При создании новых ролей необходимо обеспечить доступ к минимальному набору функциональных возможностей, которых будет достаточно для выполнения пользователями СКДПУ НТ, ассоциированными с этими ролями, своих должностных обязанностей.

СКДПУ НТ в разделе веб-интерфейса **Права доступа** предоставляет функционал, который позволяет:

- настраивать политику доступа к функциональным возможностям СКДПУ НТ;
- настраивать политику доступа к обрабатываемым данным пользовательских сессий целевых систем;
- настраивать доступ к объектам политики в целях разграничения выполняемых пользователями СКДПУ НТ возложенных на них обязанностей;
- настраивать парольную политику СКДПУ НТ;
- связать пользователей из доменов LDAP с ролями СКДПУ НТ.

4.2 Пользователи СКДПУ НТ

С помощью данного раздела администратор имеет возможность добавлять/изменять/удалять учетные записи пользователей СКДПУ НТ, предоставлять пользователям доступ к функциональным возможностям СКДПУ НТ в зависимости от их функциональных обязанностей, в том числе настраивать время, в течение которого пользователь может получить доступ к функциональным возможностям СКДПУ НТ.

В данном разделе представлена следующая информация о пользователях СКДПУ НТ (см. [рисунок 4](#)):

- (1) – уникальный идентификатор пользователя;
- (2) – ФИО пользователей СКДПУ НТ;
- (3) – электронная почта;
- (4) – ассоциированные с пользователем роли;
- (5) – настройки времени жизни учетной записи и пароля пользователя, статистика неудачных авторизаций, отметка о блокировке пользователя.

(1) Идентификатор пользователя	(2) ФИО	(3) Электронная почта	(4) Роль	Учётная запись Заблокирован	Пароль истекает	(5) Пароль истекает	Количество неудачных попыток входа	Обязательная смена пароля
User	Ivan Ivanov	user@e-mail.com	Operator	Да	2019-12-07	2020-11-26	1	Да
odminko	Ya Odminko	od@min.ko	Administrator	Нет	Никогда	2020-11-18	0	Да
root			Administrator	Нет	Никогда	Никогда	2	Нет
someadmin		mds@it-bastion.com	Administrator	Нет	Никогда	Никогда	1	Да
test123	test tester	mds@it-bastion.com	Administrator	Нет	Никогда	2020-11-15	1	Да
op	admin	e@ma.il	Operator	Нет	Никогда	2020-11-26	1	Да
mds@test.local			test-role, Administrator	Нет	Никогда	Никогда	0	Нет
root@test.local			test-role	Нет	Никогда	Никогда	0	Нет
User_sys		user@e-mail.com	System administrator	Нет	Никогда	Никогда	0	Да

Рисунок 4 – Раздел Права доступа > Пользователи

4.2.1 Добавление учетной записи пользователя СКДПУ НТ

Чтобы добавить нового пользователя СКДПУ НТ необходимо:

Шаг 1. В разделе **Права доступа>Пользователи** нажать  **Добавить пользователя**.

Шаг 2. В появившейся форме ввести необходимую информацию о пользователе

Добавить пользователя

Идентификатор пользователя (1)

ФИО (2)

Пароль (3)

Подтверждение пароля (4)

Пароль истекает (5)

Учётная запись истекает (6)

Электронная почта (7)

Роль (8)

Язык (9) Русский Английский Французский Немецкий

Заблокирован (10)

Обязательная смена пароля (11)

Сохранить

- (1) – логин пользователя;
- (2) – ФИО пользователя;
- (3) – пароль учетной записи пользователя;



Параметры пароля задаются в разделе **Права доступа > Парольная политика**.

- (4) – подтверждение пароля учетной записи пользователя;
- (5) – дата окончания действия пароля;



По умолчанию время действия пароля (5) устанавливается сроком на 365 дней с момента даты создания нового пользователя СКДПУ НТ.

- (6) – дата окончания доступа к учетной записи пользователя;



Если дата окончания доступа не установлена, то срок действия учетной записи не ограничен.

- (7) – адрес электронной почты пользователя;
- (8) – роль, с которой ассоциируется пользователь;
- (9) – язык веб-интерфейса СКДПУ НТ;
- (10) – отметка о блокировке учетной записи пользователя;
- (11) – отметка об обязательной смене пароля при первом входе после регистрации учетной записи.



Поля (1), (3), (4), (7), (8) являются обязательными для заполнения, иначе происходит оповещение пользователя об ошибке.

Шаг 3. Для сохранения внесенных данных необходимо нажать **Сохранить**.

При успешном добавлении учетной записи пользователя появится оповещение

Пользователь добавлен

4.2.2 Удаление учетной записи пользователя СКДПУ НТ

Чтобы удалить пользователя СКДПУ НТ необходимо:

Шаг 1. Нажать **✕** в строке пользователя из списка в разделе **Права доступа>Пользователи**:

User	Ivan Ivanov	user@e-mail.com	Operator	Да	2019-12-07	2020-11-26	1	Да	✕
------	-------------	-----------------	----------	----	------------	------------	---	----	---

Шаг 2. Назначить нового ответственного за проведение расследования инцидентов, ответственным за которые был удаляемый пользователь

Укажите ответственного вместо удаляемого пользователя

Выберите владельца инцидента

Отмена

Удалить

Шаг 3. Подтвердить удаление учетной записи пользователя нажатием **Удалить**

При успешном удалении учетной записи пользователя появится оповещение

Пользователь удален

4.2.3 Редактирование данных учетной записи пользователя СКДПУ НТ


Чтобы изменить данные существующего пользователя СКДПУ НТ необходимо:

Шаг 1. Выбрать пользователя из списка в разделе **Права доступа>Пользователи** нажатием левой кнопки мыши:

User	Ivan Ivanov	user@e-mail.com	Operator	Да	2019-12-07	2020-11-26	1	Да	✕
------	-------------	-----------------	----------	----	------------	------------	---	----	---



Пользователь ✕ Редактировать



Идентификатор пользователя: User
ФИО: Ivan Ivanov
Электронная почта: user@e-mail.com
Роль: Operator
Заблокирован: Да
Учётная запись истекает: 2019-12-07
Пароль истекает: 2020-11-26
Количество неудачных попыток входа: 1
Обязательная смена пароля: Да
Зарегистрирован: 2019-10-16 16:47:43
Последний вход в: 2019-12-06 13:35:22
Последний неудачный вход в: 2020-04-29 16:42:42
Язык: ru

Шаг 2. Нажать **Редактировать**.

Шаг 3. В появившейся форме изменить необходимую информацию о пользователе:

Редактировать пользователя

Идентификатор пользователя
user

ФИО
Ivan Ivanov

Пароль
Оставьте это поле пустым для сохранения текущего пароля

Подтверждение пароля

Пароль истекает
2020-11-26

Учётная запись истекает
2019-12-17

Количество неудачных попыток входа
0

Электронная почта
user@e-mail.com

Роль
Operator

Язык
 Русский Английский Французский Немецкий

Заблокирован

Обязательная смена пароля

Сохранить



Подробнее о полях см. [раздел 4.2.1](#).

Шаг 4. Для сохранения внесенных изменений необходимо нажать **Сохранить**.

При успешном изменении данных учетной записи пользователя появится оповещение

Пользователь обновлен x

4.2.3.1 Изменение пароля пользователя СКДПУ НТ

Чтобы изменить пароль пользователя СКДПУ НТ необходимо:

Шаг 1. Открыть форму для редактирования данных пользователя (см. [раздел 4.2.3](#)).

Шаг 2. В соответствующее поле ввести пароль и повторить его еще раз:

Пароль

Оставьте это поле пустым для сохранения текущего пароля

Подтверждение пароля



Пароль должен соответствовать парольной политике, которая задается в разделе 4.5.

Шаг 3. Для сохранения внесенных изменений необходимо нажать **Сохранить**.

При успешном изменении данных учетной записи пользователя появится оповещение

Пользователь обновлен x

4.2.3.2 Блокирование/разблокирование учетной записи пользователя СКДПУ НТ

Чтобы заблокировать/разблокировать существующего пользователя СКДПУ НТ необходимо:

Шаг 1. Открыть форму для редактирования данных пользователя (см. раздел 4.2.3).

Шаг 2. В появившейся форме выделить **Заблокирован** или снять выделение **Заблокирован** для блокирования или разблокирования пользователя СКДПУ НТ соответственно.



Если пользователь превысил установленное кол-во неуспешных попыток аутентификации, то перед снятием блокировки пользователя следует обнулить кол-во неуспешных попыток нажатием

Количество неудачных попыток входа

Шаг 3. Для сохранения внесенных изменений необходимо нажать **Сохранить**.

При успешном изменении данных учетной записи пользователя появится оповещение

Пользователь обновлен x

4.2.3.3 Изменение срока действия учетной записи и пароля пользователя СКДПУ НТ

Установить время жизни учетной записи и пароля пользователя СКДПУ НТ можно при создании нового пользователя (см. раздел 4.2.1) или при внесении изменений в настройки учетной записи уже существующего пользователя СКДПУ НТ (см. раздел 4.2.3).

Необходимо выполнить следующие шаги:

Шаг 1. В соответствующие поля при создании пользователя (см. раздел 4.2.1) или при изменении данных уже существующего пользователя (см. раздел 4.2.3) ввести

желаемые даты окончания действия учетной записи и пароля пользователя СКДПУ НТ:

Пароль истекает

2020-11-26

Учётная запись истекает

2020-11-26

Шаг 2. Для сохранения внесенных изменений необходимо нажать **Сохранить**.

При успешном изменении данных учетной записи пользователя появится оповещение

Пользователь обновлен X

4.2.4 Доменный пользователь СКДПУ НТ

Для добавления доменного пользователя необходимо привязать группу LDAP, в которой состоит доменный пользователь, к роли СКДПУ НТ (см. [раздел 4.6](#)).



Доменный пользователь не существует в СКДПУ НТ до тех пор, пока с его учетными данными не будет осуществлен вход.

При первом успешном входе запись о доменном пользователе сохраняется в системе (добавляется в раздел **Права доступа > Пользователи**), после чего эта учетная запись принимает на себя роль группы LDAP, но при этом ее параметры невозможно редактировать.

4.3 Роли СКДПУ НТ

С помощью рассматриваемого раздела администратор имеет возможность создавать/изменять/удалять роли в целях обеспечения разграничения выполняемых пользователями обязанностей.

Также администратор имеет возможность для каждой роли через ограничение списка доступных персон, целевых систем, групп персон LDAP, групп систем LDAP настроить список ограничений на доступ к данным пользовательских сессий на целевых системах в целях разграничения доступа к обрабатываемой информации.

Отмечая разрешения на чтение, запись и выполнение, администратор тем самым дает право на доступ рассматриваемой роли к соответствующим разделам веб-интерфейса СКДПУ НТ (см. [таблицу 2](#)).

Таблица 2 – Права доступа к разделам веб-интерфейса СКДПУ НТ

Ресурс	Раздел веб-интерфейса	Права на доступ		
		Чтение	Запись	Выполнение
Аномалии	Аномалии	X	X	-
Журнал авторизаций	Отчеты>Журнал авторизаций	X	-	-
Мониторинг	Мониторинг	X	-	-

Ресурс	Раздел веб-интерфейса	Права на доступ		
		Чтение	Запись	Выполнение
Ограничения доступа к данным	Права доступа>Ограничения доступа к данным	X	X	-
Профили выполнения	Отчеты>Профили выполнения	X	X	-
Основные настройки	Настройки>Основные настройки	X	X	-
Инциденты	Инциденты	X	X	-
Настройки LDAP	Настройки>Настройки LDAP	X	X	-
Группы LDAP	Права доступа>Группы LDAP	X	X	-
Лицензия	Настройки>Информация о лицензии	X	X	-
Диагностика	Диагностика	X	-	-
Парольная политика	Права доступа>Парольная политика	X	X	-
Персоны	Персоны	X	X	-
Шлюзы	Компоненты>Шлюзы	X	X	-
Отчеты	Отчеты>Отчеты	X	X	X
История выполнения	Отчеты>История выполнения	X	X	-
Роли	Роли	X	X	-
Сессии	Сессии	X	-	-
Библиотека отчётов	Отчеты>Библиотека отчетов	X	X	X
Конфигурация журналирования	Настройки>Конфигурация журналирования	X	X	-
Системные настройки	Настройки>Системные настройки	X	X	-
Цели	Компоненты>Цели	X	-	-
Список пользователей		X	-	-
Пользователи	Пользователи	X	X	-

Каждый профиль представляет собой набор прав, для каждого из которых определен набор разрешений, необходимых для получения доступа к соответствующему объему функциональности СКДПУ НТ (см. [таблица 3](#)).

Таблица 3 – Настройка прав профилей

Право	Разрешение	Описание	Раздел веб-интерфейса
Аномалии	Чтение	Просмотр настроек детекторов аномалий	Аномалии

Право	Разрешение	Описание	Раздел веб-интерфейса
	Запись	Управление настройками детекторов аномалий	Аномалии
Журнал авторизаций	Чтение	Просмотр журнала авторизаций пользователей СКДПУ ИТ	Отчеты > Журнал авторизаций
Мониторинг	Чтение	Просмотр сводной статистики на контролируемых целевых системах	Мониторинг
Ограничения доступа к данным	Чтение	Просмотр перечня ограничений	Права доступа > Ограничение доступа к данным
	Запись	Создание записей ограничений. Для добавления персон, шлюзов и целей необходимы следующие разрешения: <ul style="list-style-type: none"> • Персоны (для добавления ограничений на просмотр персоны) • Компоненты > Шлюзы (для добавления ограничений на просмотр шлюзов) • Компоненты > Цели (для добавления ограничений на просмотр целей) 	Права доступа > Ограничение доступа к данным
Профили выполнения	Чтение	Просмотр перечня доступных текущему пользователю профилей выполнения	Отчеты > Профили выполнения
	Запись	Добавление и редактирование профилей выполнения	Отчеты > Профили выполнения
Основные настройки	Чтение	Просмотр настроек почтового сервера, отчетов и веб-приложения	Настройки > Основные настройки
	Запись	Изменение настроек почтового сервера, отчетов и веб-приложения	Настройки > Основные настройки
Запись	Добавление и редактирование белых списков инцидентов	Аномалии > Настройки белых списков	
Инциденты	Чтение	Просмотр таблицы инцидентов и возможность просмотра информации о выбранном инциденте	Инциденты

Право	Разрешение	Описание	Раздел веб-интерфейса
	Запись	Для назначения ответственного за расследование инцидента необходимо разрешение Права доступа > Пользователи	Инциденты
Настройки LDAP	Чтение	Просмотр настроек доменов LDAP	Настройки > Настройки LDAP
	Запись	Управление подключением доменов LDAP	Настройки > Настройки LDAP
Группы LDAP	Чтение	Просмотр доступных для привязки групп пользователей в домене LDAP	Права доступа > Группы LDAP
	Запись	Управление привязкой групп пользователей к ролям СКДПУ ИТ	Права доступа > Группы LDAP
Лицензия	Чтение	Просмотр информации о текущей лицензии	Настройки > Информация о лицензии
	Запись	Управление (загрузка и выгрузка) лицензией	Настройки > Информация о лицензии
Диагностика	Чтение	Просмотр данных о потреблении системных ресурсов, управление процессами СКДПУ ИТ, просмотр информации о текущей лицензии и сборке СКДПУ ИТ	Диагностика
Парольная политика	Чтение	Просмотр текущей парольной политики СКДПУ ИТ	Права доступа > Парольная политика
	Запись	Управление парольной политикой СКДПУ ИТ	Права доступа > Парольная политика
Персоны	Чтение	Просмотр перечня доступных персон (пользователей целевых систем)	Персоны
	Запись	Добавление дополнительной информации о персонах в целях их идентификации	Персоны
Шлюзы	Чтение	Просмотр информации о подключенных шлюзах доступа	Компоненты > Шлюзы
	Запись	Настройка доступа к данным пользовательских сессий, которые хранятся на соответствующих шлюзах доступа	Компоненты > Шлюзы
Отчёты	Чтение	Просмотр принадлежащих текущему пользователю отчетов	Отчеты > Отчеты
	Запись	Редактирование и удаление выбранного отчета	Отчеты > Отчеты

Право	Разрешение	Описание	Раздел веб-интерфейса
	Выполнение	Генерирование выбранного отчета через веб-интерфейс	Отчеты > Отчеты
История выполнения	Чтение	Просмотр сгенерированных отчетов, принадлежащих текущему пользователю	Отчеты > История выполнения
	Запись	-	Отчеты > История выполнения
Роли	Чтение	Просмотр перечень ролей СКДПУ НТ	Права доступа > Роли
	Запись	Создание, редактирование и удаление ролей СКДПУ НТ	Права доступа > Роли
Сессии	Чтение	Просмотр пользовательских сессий целевых систем	Сессии
Библиотека отчетов	Чтение	Просмотр перечня шаблонов отчетов	Отчеты > Библиотека отчетов
	Запись	-	Отчеты > Библиотека отчетов
	Выполнение	Предварительный просмотр данных отчета. Создание отчетов на базе доступного перечня шаблонов происходит при условии, что есть разрешение Отчеты > Запись . Выбор профиля выполнения осуществляется при условии, что есть разрешение Профили выполнения > Чтение	Отчеты > Библиотека отчетов
Конфигурация журналирования	Чтение	Просмотр перечня подключений к серверам, куда передаются данные журналов аудита СКДПУ НТ	Настройки > Конфигурация журналирования
	Запись	Управление подключениями к серверам, куда передаются данные журналов аудита СКДПУ НТ	Настройки > Конфигурация журналирования
Системные настройки	Чтение	Просмотр системных настроек и настроек хранения данных СКДПУ НТ по умолчанию (инцидентов, пользовательских сессий целевых систем, целей, персон, архивов)	Настройки > Системные настройки
	Запись	Управление системными настройками и настройками хранения данных СКДПУ НТ по умолчанию (инцидентов, пользовательских сессий целевых систем, целей, персон, архивов)	Настройки > Конфигурация журналирования

Право	Разрешение	Описание	Раздел веб-интерфейса
Цели	Чтение	Просмотр перечня целей (устройств), к которым осуществлялся доступ	Компоненты > Цели
Список пользователей	-	-	-
Пользователи	Чтение	Просмотр перечня пользователей СКДПУ НТ	Права доступа > Пользователи
	Запись	Управление учетными записями пользователей СКДПУ НТ	Права доступа > Пользователи

СКДПУ НТ содержит следующие встроенные роли, которые невозможно модифицировать:

- Администратор СКДПУ НТ, который имеет неограниченный доступ ко всем функциям СКДПУ НТ. Отвечает за установку и первичную настройку конфигурации СКДПУ НТ. Осуществляет управление доступом к функционалу СКДПУ НТ. Может создавать новые роли пользователей.

Ресурс	Чтение	Запись	Выполнение
Аномалии	✓	✓	
Журнал авторизаций	✓		
Мониторинг	✓		
Ограничения доступа к данным	✓	✓	
Профили выполнения	✓	✓	
Основные настройки	✓	✓	
Белый список инцидентов	✓	✓	
Инциденты	✓	✓	
Настройки LDAP	✓	✓	
Группы LDAP	✓	✓	
Лицензия	✓	✓	
Диагностика	✓		✓
Парольная политика	✓	✓	
Персоны	✓	✓	
Шлюзы	✓	✓	
Отчёты	✓	✓	✓
История выполнения	✓	✓	
Роли	✓	✓	
Сессии	✓		
Библиотека отчётов	✓		✓
Конфигурация журналирования	✓	✓	
Системные настройки	✓	✓	
Цели	✓		
Список пользователей	✓		
Пользователи	✓	✓	

- Системный администратор СКДПУ НТ, который осуществляет настройку и диагностику СКДПУ НТ в процессе эксплуатации. Данная роль не имеет штатного доступа к данным пользовательских сессий на целевых системах.

Ресурс	Чтение	Запись	Выполнение
Основные настройки	✓	✓	
Белый список инцидентов	✓	✓	
Настройки LDAP	✓	✓	
Лицензия	✓	✓	
Диагностика	✓		✓
Конфигурация журналирования	✓	✓	
Системные настройки	✓	✓	
Список пользователей	✓		

- Оператор СКДПУ НТ, который в процессе эксплуатации осуществляет просмотр данных пользовательских сессий, управление инцидентами и отвечает за конфигурацию генерируемых отчетов.

Ресурс	Чтение	Запись	Выполнение
Мониторинг	✓		
Профили выполнения	✓	✓	
Белый список инцидентов	✓	✓	
Инциденты	✓	✓	
Лицензия	✓	✓	
Персоны	✓		
Шлюзы	✓		
Отчёты	✓	✓	✓
История выполнения	✓	✓	
Сессии	✓		
Библиотека отчётов	✓		✓
Цели	✓		
Список пользователей	✓		

В рассматриваемом разделе представлена следующая информация о ролях СКДПУ НТ (см. рисунок 5):

- (1) – уникальный идентификатор роли;
- (2) – количество разрешений на доступ к функциональным возможностям СКДПУ НТ у соответствующих ролей;
- (3) – количество групп LDAP, ассоциированных с соответствующими ролями (см. Группы LDAP);
- (4) – количество ограничений на доступ к данным пользовательских сессий целевых систем у соответствующих ролей;
- (5) – количество пользователей, ассоциированных с соответствующими ролями.

(1) Роль	(2) Разрешения	(3) Группы LDAP	(4) Ограничения доступа к данным	(5) Пользователи
Administrator	21	1	0	20
Operator	12	0	0	2
System administrator	6	0	0	1

Рисунок 5 – Раздел Права доступа > Роли

4.3.1 Добавление новой роли

Чтобы добавить роль СКДПУ НТ необходимо:

Шаг 1. В разделе **Права доступа>Роли** нажать [Добавить роль](#).

Шаг 2. В появившейся форме отметить желаемые разрешения на доступ к функционалу интерфейса СКДПУ НТ

Роль

Муроль

Разрешения

Ресурс	Чтение	Запись	Выполнение
Аномалии	<input type="checkbox"/>	<input type="checkbox"/>	
Журнал авторизаций	<input type="checkbox"/>		
Мониторинг	<input type="checkbox"/>		
Ограничения доступа к данным	<input type="checkbox"/>	<input type="checkbox"/>	
Профили выполнения	<input type="checkbox"/>	<input type="checkbox"/>	
Основные настройки	<input type="checkbox"/>	<input type="checkbox"/>	
Белый список инцидентов	<input type="checkbox"/>	<input type="checkbox"/>	
Инциденты	<input type="checkbox"/>	<input type="checkbox"/>	
Настройки LDAP	<input type="checkbox"/>	<input type="checkbox"/>	
Группы LDAP	<input type="checkbox"/>	<input type="checkbox"/>	
Лицензия	<input type="checkbox"/>	<input type="checkbox"/>	
Диагностика	<input type="checkbox"/>		
Парольная политика	<input type="checkbox"/>	<input type="checkbox"/>	
Персоны	<input type="checkbox"/>	<input type="checkbox"/>	
Шлюзы	<input type="checkbox"/>	<input type="checkbox"/>	
Отчёты	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
История выполнения	<input type="checkbox"/>	<input type="checkbox"/>	
Роли	<input type="checkbox"/>	<input type="checkbox"/>	
Сессии	<input type="checkbox"/>		
Библиотека отчётов	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Конфигурация журналирования	<input type="checkbox"/>	<input type="checkbox"/>	
Системные настройки	<input type="checkbox"/>	<input type="checkbox"/>	
Цели	<input type="checkbox"/>		
Список пользователей	<input type="checkbox"/>		
Пользователи	<input type="checkbox"/>	<input type="checkbox"/>	

Ограничения доступа к данным

a
test_restr

[Сохранить](#)

Шаг 3. Выбрать группу ограничений доступа к данным (см. [раздел 4.4](#)).

Шаг 4. Для сохранения внесенных данных необходимо нажать [Сохранить](#).

При успешном добавлении роли появится оповещение

Роль успешно создана x

4.3.2 Редактирование разрешений для существующей роли

Для редактирования роли СКДПУ НТ необходимо:

Шаг 1. Выбрать роль из списка в разделе **Права доступа**>**Роли** нажатием левой кнопки мыши:

Роль	Разрешения	Группы LDAP	Ограничения доступа к данным	Пользователи
Administrator	21	1	0	20
MyRole	0	0	0	0
Operator	12	0	1	1



←
Напечатать
✎ Редактировать

Роль: MyRole

Ресурс	Чтение	Запись	Выполнение

Шаг 2. Нажать ✎ Редактировать.

Шаг 3. В появившейся форме внести изменения:

← Роль MyRole ↗

Роль: MyRole

Разрешения

Ресурс	Чтение	Запись	Выполнение
Аномалии	<input type="checkbox"/>	<input type="checkbox"/>	
Журнал авторизаций	<input type="checkbox"/>		
Мониторинг	<input type="checkbox"/>		
Ограничения доступа к данным	<input type="checkbox"/>	<input type="checkbox"/>	
Профили выполнения	<input type="checkbox"/>	<input type="checkbox"/>	
Основные настройки	<input type="checkbox"/>	<input type="checkbox"/>	
Инциденты	<input type="checkbox"/>	<input type="checkbox"/>	
Настройки LDAP	<input type="checkbox"/>	<input type="checkbox"/>	
Диагностика	<input type="checkbox"/>		
Персоны	<input type="checkbox"/>	<input type="checkbox"/>	
Шлюзы	<input type="checkbox"/>	<input type="checkbox"/>	
Отчёты	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
История выполнения	<input type="checkbox"/>	<input type="checkbox"/>	
Роли	<input type="checkbox"/>	<input type="checkbox"/>	
Сессии	<input type="checkbox"/>		
Библиотека отчётов	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Конфигурация журналирования	<input type="checkbox"/>	<input type="checkbox"/>	
Системные настройки	<input type="checkbox"/>	<input type="checkbox"/>	
Цели	<input type="checkbox"/>		
Список пользователей	<input type="checkbox"/>		
Пользователи	<input type="checkbox"/>	<input type="checkbox"/>	

Ограничения доступа к данным

1q1q1q
test
testik

Сохранить

Шаг 4. Для сохранения внесенных изменений необходимо нажать Сохранить.

При успешном сохранении роли появится оповещение

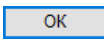
Роль обновлена успешно x

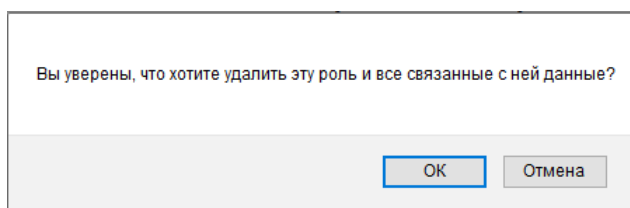
4.3.3 Удаление существующей роли

Чтобы удалить роль СКДПУ НТ необходимо, чтобы данная роль не ассоциировалась ни с одним из пользователей СКДПУ НТ:

Шаг 1. Нажать  в строке роли из списка в разделе **Права доступа>Роли**:

Роль	Разрешения	Группы LDAP	Ограничения доступа к данным	Пользователи
Administrator	21	1	0	20
MyRole	0	0	0	0
Operator	12	0	1	1

Шаг 2. Подтвердить удаление учетной записи пользователя нажатием  в диалоговом окне

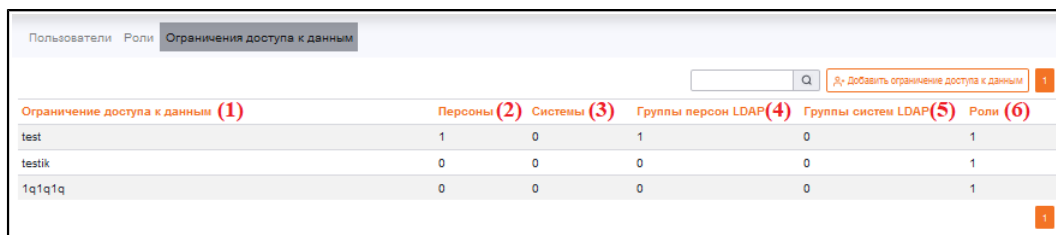


4.4 Управление доступом к данным

С помощью данного раздела администратор СКДПУ НТ имеет возможность создавать, изменять и удалять ограничения на доступ к данным пользовательских сессий на целевых системах, разграничивать доступ к данным пользовательских сессий на целевых системах, определяя границы ответственности уполномоченных пользователей СКДПУ НТ по мониторингу пользовательских сессий на предмет обнаружения и последующей обработке инцидентов информационной безопасности через определение доступных пользователю персон, целевых систем, групп пользователей LDAP, групп систем LDAP.

В рассматриваемой вкладке представлена следующая информация об ограничениях доступа к данным пользовательских сессий на целевых системах (см. [рисунок 6](#)):

- (1) – уникальный идентификатор ограничения доступа к данным пользовательских сессий целевых систем;
- (2) – количество персон, включенных в перечень для осуществления мониторинга;
- (3) – количество целевых систем, включенных в перечень для осуществления мониторинга;
- (4) – количество групп LDAP, включенных в перечень для осуществления мониторинга;
- (5) – количество групп LDAP, включенных в перечень мониторинга;
- (6) – количество ролей, ассоциированных с соответствующими ограничениями.



Ограничение доступа к данным (1)	Персоны (2)	Системы (3)	Группы персон LDAP (4)	Группы систем LDAP (5)	Роли (6)
test	1	0	1	0	1
testik	0	0	0	0	1
1q1q1q	0	0	0	0	1

Рисунок 6 – Раздел Права доступа > Ограничения доступа к данным

В СКДПУ НТ администратору предоставляется возможность составить списки ограничения на доступ к данным пользовательских сессий на целевых системах. Для формирования списков необходимо указать целевые системы и их пользователей для мониторинга их деятельности. Идентификаторы систем и персон могут определяться двумя способами:

- идентификаторы определены средствами самих целевых систем;
- идентификаторы определены с помощью информации, содержащейся в структурах LDAP-доменов.

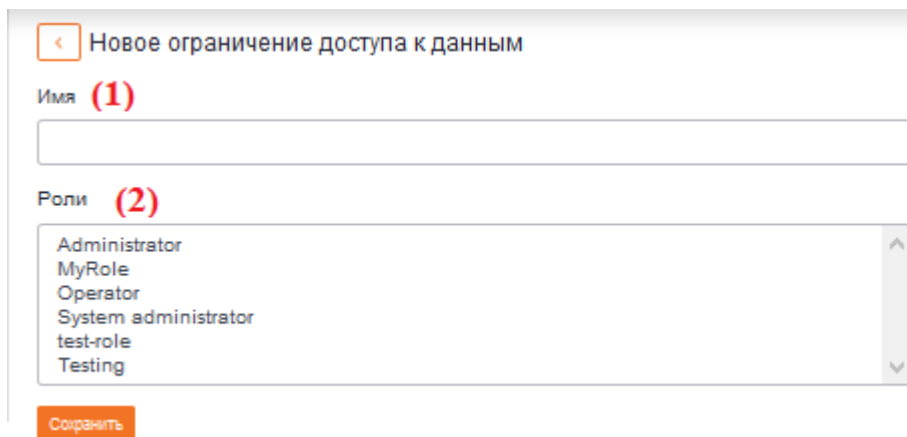
4.4.1 Создание ограничения доступа к данным

Для создания ограничения доступа к данным необходимо:

Шаг 1. Перейти в раздел **Права доступа>Ограничения доступа к данным**

Шаг 2. Нажать 

- Шаг 3. В появившейся форме необходимо ввести идентификатор ограничения (1) и, если необходимо, выбрать роли, на которые будет распространяться создаваемое ограничение (2)



Новое ограничение доступа к данным

Имя (1)

Роли (2)

- Administrator
- MyRole
- Operator
- System administrator
- test-role
- Testing

Сохранить



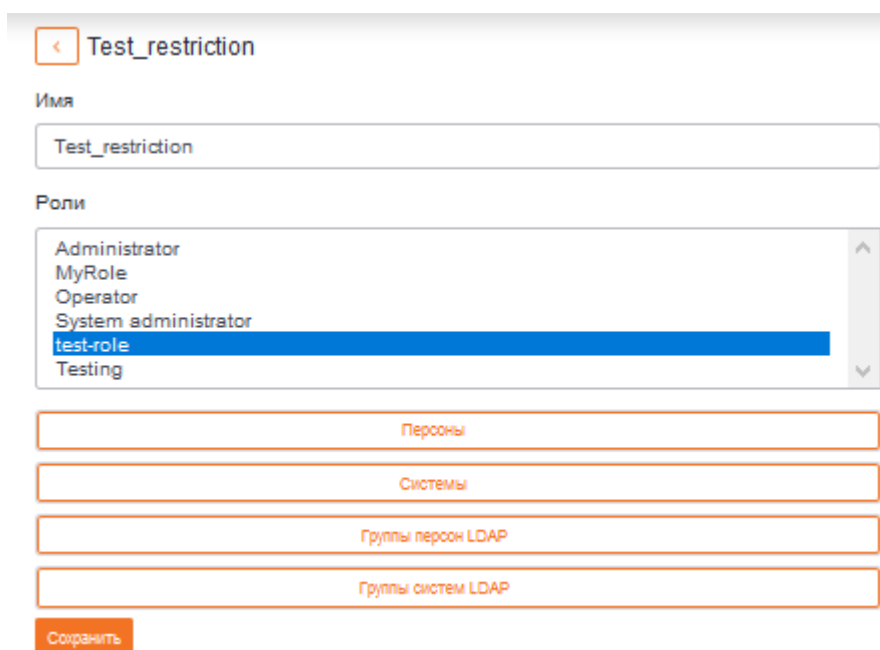
Для выбора нескольких ролей необходимо зажать **Ctrl** и левой кнопкой мыши указать желаемые роли.



Для снятия выделения с роли необходимо зажать **Ctrl** и левой кнопкой мыши указать роль из списка.

- Шаг 4. Нажать **Сохранить** для перехода к формированию списков ограничений.

- Шаг 5. В появившейся форме можно сформировать списки ограничений на доступ к данным (см. [раздел 4.4.3](#))



Test_restriction

Имя

Test_restriction

Роли

- Administrator
- MyRole
- Operator
- System administrator
- test-role
- Testing

Персоны

Системы

Группы персон LDAP

Группы систем LDAP

Сохранить

Шаг 6. Для сохранения нового ограничения следует нажать **Сохранить**.

4.4.2 Редактирование ограничения доступа к данным

Для редактирования ограничения доступа к данным необходимо:

Шаг 1. Перейти в раздел **Права доступа>Ограничения доступа к данным**

Шаг 2. Выбрать роль из списка в разделе **Права доступа>Ограничения доступа к данным** нажатием левой кнопки мыши

Ограничение доступа к данным	Персоны	Системы	Группы персон LDAP	Группы систем LDAP	Роли
Test_restriction	0	0	0	0	1

Имя

Роли

- Administrator
- MyRole**
- Operator
- System administrator
- test-role
- Testing

Сохранить

Шаг 3. В появившейся форме можно изменить количество ролей, на которые будет действовать редактируемое ограничение, (см. [раздел 4.4.1](#)) или выбрать необходимую категорию объектов для их включения в списки ограничения доступа (см. [раздел 4.4.3](#)).

Шаг 4. Для сохранения внесенных изменений необходимо нажать **Сохранить**.

4.4.3 Формирование списков ограничения доступа к данным

Для формирования списков ограничения доступа к данным в независимости от объектов, которые будут включены в эти списки, необходимо:

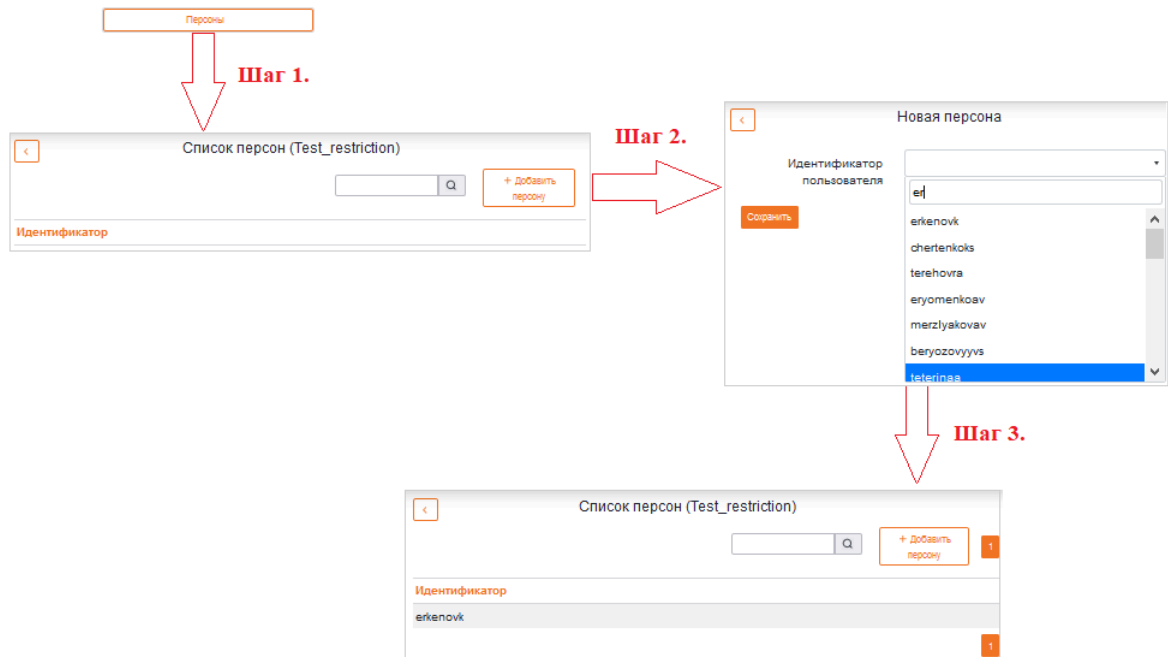
Шаг 1. Выбрать соответствующую категорию объектов.

Шаг 2. В появившейся форме добавить соответствующий объект.

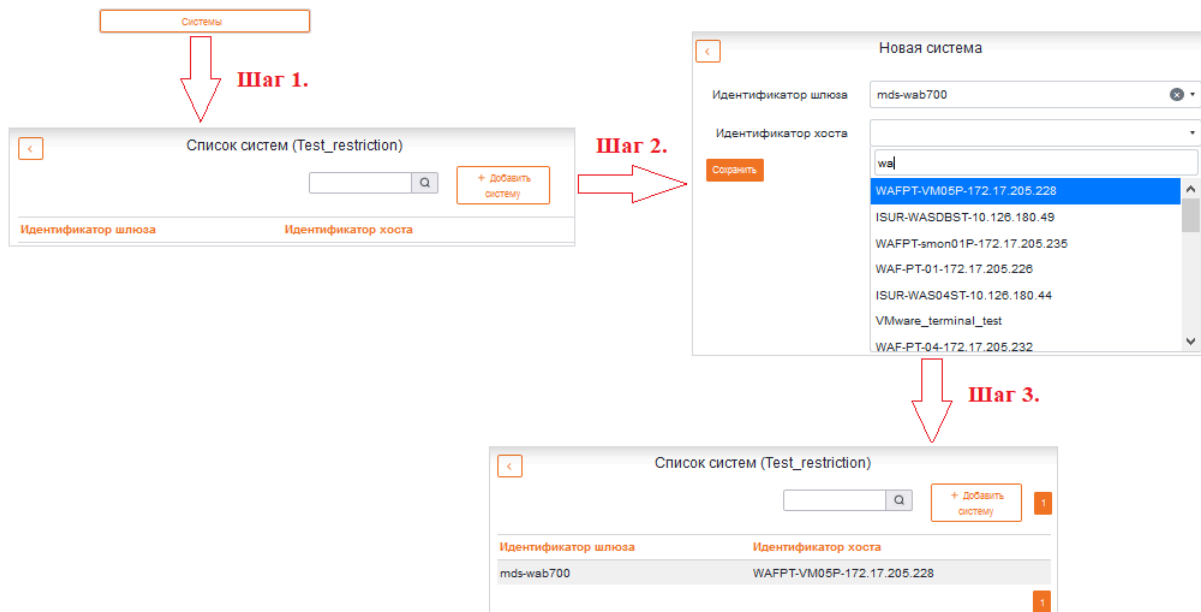
Шаг 3. Заполнить необходимые поля и зафиксировать данные нажатием **Сохранить**.

Далее рассмотрены примеры заполнения списков каждой из категорий.

Добавление персоны



Добавление системы



Добавление группы персон LDAP

Группы персон LDAP

Шаг 1.

Список групп персон LDAP (Test_restriction)

Имя	Описание	Домен
-----	----------	-------

Шаг 2.

Новая группа персон LDAP

Домен:

Группа LDAP:

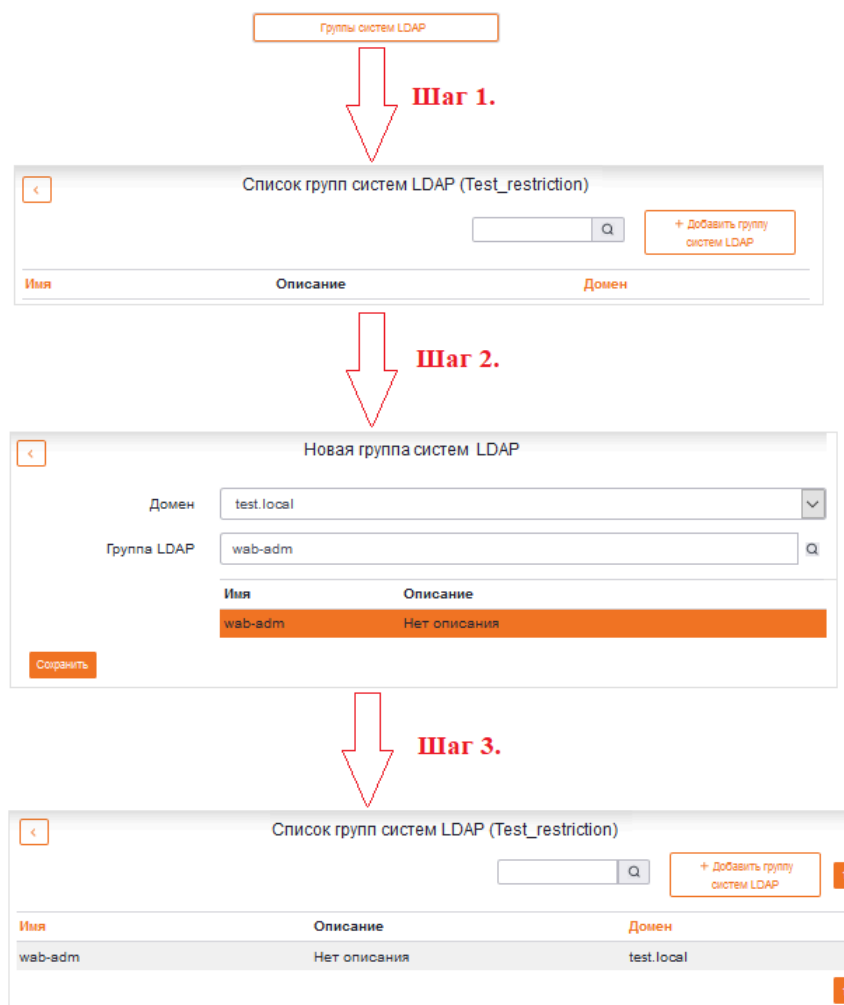
Имя	Описание
wab-adm	Нет описания

Шаг 3.

Список групп персон LDAP (Test_restriction)

Имя	Описание	Домен
wab-adm	Нет описания	test.local

Добавление группы систем LDAP



4.4.4 Удаление ограничения доступа к данным

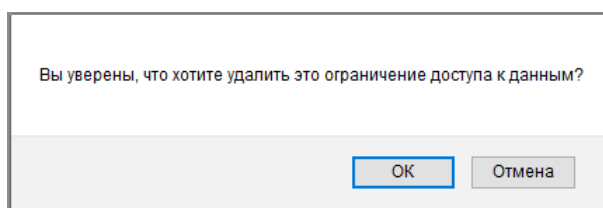
Для удаления ограничения доступа к данным необходимо:

Шаг 1. Перейти в раздел **Права доступа**>**Ограничения доступа к данным**

Шаг 2. Нажать  в строке ограничения из списка:

Ограничение доступа к данным	Персоны	Системы	Группы персон LDAP	Группы систем LDAP	Роли
test	1	1	2	0	1
testik	0	0	0	0	1
1q1q1q	0	0	0	0	2

Шаг 3. Подтвердить удаление ограничения нажатием  в диалоговом окне





Если никакое ограничение не назначено, то пользователю доступны все объекты для получения информации. Если назначено хотя бы одно ограничения, то пользователю будет предоставлен доступ к информации только по этому объекту политики.

4.5 Управление парольной политикой пользователей СКДПУ НТ

Для настройки парольной политики необходимо:

Шаг 1. Перейти в раздел **Права доступа**>**Парольная политика**

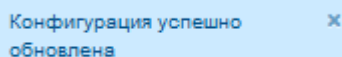
Шаг 2. Нажать на  **Редактировать**

Шаг 3. В появившейся форме внести изменения в следующие настройки:

- минимальная длина пароля;
- максимальная длина пароля;
- минимальное количество строчных символов;
- минимальное количество заглавных символов;
- минимальное количество цифровых символов;
- минимальное количество специальных символов (~, !, @, #, \$ и т.д.);
- отметка о несовпадении пароля и идентификатора пользователя СКДПУ НТ;
- время действия пароля (указывается в днях);
- предупреждение пользователя СКДПУ НТ об окончании действия пароля (указывается в днях);
- максимальное количество попыток ввода пароля до блокирования учетной записи пользователя СКДПУ НТ;
- количество предыдущих паролей, запрещенных для повторного использования.

Шаг 4. Чтобы зафиксировать внесенные изменения, необходимо нажать  **Сохранить**.

При успешном сохранении настроек появится оповещение



Конфигурация успешно обновлена

4.6 Группы LDAP

СКДПУ НТ предоставляет возможность назначить роли СКДПУ НТ пользователям доменов LDAP, для этого необходимо:

Шаг 1. Перейти в раздел веб-интерфейса **Права доступа**>**Группы LDAP**.

[Редактировать](#)

Группы LDAP	
test.local (по умолчанию)	
Administrators	Не связано
Denied RODC Password Replication Group	Не связано
Domain Admins	Не связано
Remote Desktop Users	Не связано
wab-adm	role-test
wab-users	Operator

Шаг 2. Нажать на [Редактировать](#).

Группы LDAP

Группы LDAP

test.local (по умолчанию)

Все группы
Роль для любой группы этого домена

Administrators
Administrators have complete and unrestricted access to the computer/domain
[Не связано](#)

Denied RODC Password Replication Group
Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain
[Не связано](#)

Domain Admins
Designated administrators of the domain
[Не связано](#)

Remote Desktop Users
Members in this group are granted the right to logon remotely
[Не связано](#)

wab-adm
Нет описания
[Связан с: role-test](#)

wab-users
Нет описания
[Связан с: Operator](#)

[Сохранить](#)

Шаг 3. Выбрать группу пользователей, которой необходимо назначить роль СКДПУ НТ

Domain Admins
Designated administrators of the domain
[Не связано](#)

[Привязать роль](#) [Отвязать роль](#)

Шаг 4. Из выпадающего списка выбрать необходимую роль и привязать к группе пользователей нажатием на [Привязать роль](#)

Шаг 5. Сохранить изменения [Сохранить](#)

При успешном сохранении настроек появится оповещение

Конфигурация успешно обновлена



Если будет необходимо отвязать роль, то следует нажать на [Отвязать роль](#)

5 ДЕТЕКТОРЫ АНОМАЛИЙ

5.1 Общие сведения

В рамках СКДПУ НТ реализованы механизмы контроля аномального поведения персон на основе применения детекторов. Под аномальным поведением следует понимать нехарактерные для пользователя используемые команды, время начала и окончание работы и т.д. В рамках СКДПУ НТ любое аномальное поведение определяется как инцидент.

В рамках СКДПУ НТ используются следующие детекторы аномального поведения:

- Детектирование потенциально опасных команд;
- Детектирование принудительного блокирования сессий;
- Контроль привычного времени работы;
- Контроль изменения уровня доверия;
- Контроль стандартных команд;
- Контроль привычных сетевых адресов;
- Контроль эффективности работы;
- Индикаторы взрывной активности;
- Детектор новых доступов;
- Детектор проблем с правами доступа к файлам;
- Детектор туннелей и прыжков;
- Детектор входов помимо бастиона;
- Анализатор ошибок авторизации;
- Детектор забытых персон;
- Количество переданных файлов;
- Детектор сканеров.

Ключевые настройки возможно изменить в разделе **Аномалии** (см. [рисунок 7](#)).

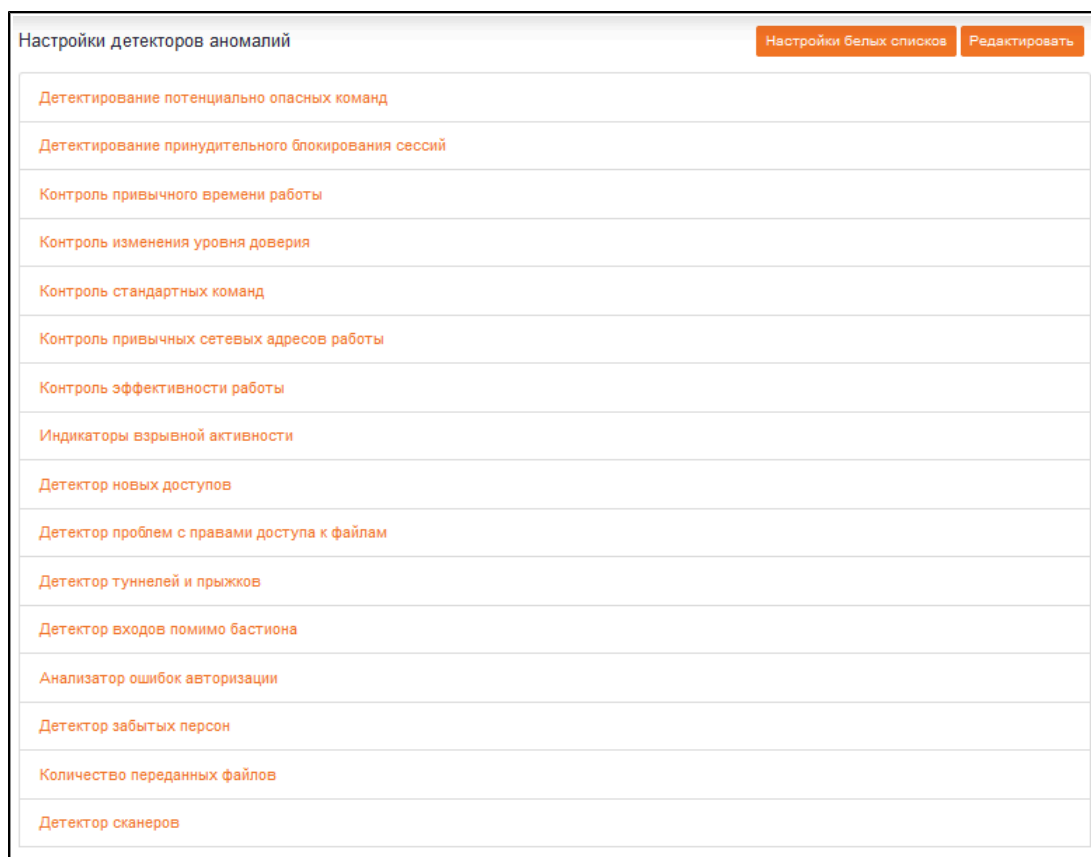


Рисунок 7 – Настройки детекторов аномалий

СКДПУ НТ предоставляет администратору возможность настраивать детекторы в целях повышения эффективности обнаружения инцидентов информационной безопасности и своевременного реагирования на них.

Для редактирования настроек детекторов необходимо нажать [Редактировать](#).

Каждый детектор возможно как отключить полностью, отключив [Активировать](#).



В текущей версии СКДПУ НТ группы персон нельзя задать, и по умолчанию детекторы применяются ко всем персонам, к информации о которых есть доступ СКДПУ НТ.

При настройке детекторов администратору СКДПУ НТ необходимо установить уровень критичности генерируемого соответствующим детектором инцидента. Уровень критичности определятся администратором с учетом результатов анализа последствий возникновения того или иного инцидента. Процедура проведения анализа критичности инцидентов обычно прописана в руководящих документах эксплуатирующей организации по управлению инцидентами и в настоящем руководстве не рассматривается.

Также администратору для каждого детектора необходимо установить численное значение весового коэффициента, определяющего условный вклад генерируемого им инцидента, который тот вносит в рассчитываемый для каждой персоны уровень доверия.

Чтобы зафиксировать внесенные изменения необходимо нажать [Сохранить](#).

5.2 Детектирование потенциально опасных команд

Рассматриваемый детектор позволяет контролировать вводимые **Персоной** команды, которые могут привести к негативным последствиям в целевой системе. Использование такого рода команд не всегда является признаком нарушения, но их выполнение может быть критично как для функционирования целевой системы в целом, так и для безопасности хранимой и обрабатываемой в ней информации.

Детектор в процессе своей работы выделяет использование **Персоной** потенциально опасных команд и сохраняет их. В случае если в рамках пользовательской сессии целевых систем было выполнено несколько потенциально опасных команд, то СКДПУ НТ может создать несколько инцидентов на одну сессию.

Детектор поддерживает проверку на ключевые последовательности событий запуска процессов.

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – перечень групп **Персон**, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (3) – названия списков;
- (4) – весовые коэффициенты для каждого из списков;
- (5) – шаблоны запрещенных команд в формате регулярных выражений.

The screenshot shows a configuration interface for a detector. At the top, there is a checkbox labeled "Активировать" (Activate) which is checked. Below it, there are two main configuration blocks, each representing a rule. Red numbers (1) through (5) are placed over the interface to indicate the locations of the parameters mentioned in the text above.

- Rule 1:**
 - Уровень (Level): Низкий (Low) - (1)
 - Группы (Groups): * - (2)
 - Название списка (List Name): black - (3)
 - Коэффициент (Coefficient): 2.0 - (4)
 - Шаблоны (Templates):
 - ^m -r
 - .*crypt.*
 - .*delete.*
 - .*hyena.*
 - .*mimikatz.*- (5)
- Rule 2:**
 - Название списка (List Name): gray - (3)
 - Коэффициент (Coefficient): 0.2 - (4)
 - Шаблоны (Templates):
 - ls /etc.*
 - .*passwd.*
 - .*Delete.*
 - .*conf.t.*
 - .*alter.table.*- (5)

At the bottom of the interface, there is a "Сохранить" (Save) button.

Рассматриваемый детектор генерирует инциденты типа «Подозрительные команды».

5.3 Детектирование принудительного блокирования сессий

Рассматриваемый детектор позволяет фиксировать факт принудительного закрытия пользовательских сессий целевых систем при обнаружении команд из черных списков, заданных в политике безопасности шлюзов доступа.

Детектор будет выделять такие события, чтобы пользователь СКДПУ ИТ знал, что сработало правило черного списка, и это может быть дополнительно расследовано.

Активировать

Уровень

Низкий (1)

Группы

* (2)

Коэффициент

1.6 (3)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – перечень групп **Персон**, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (3) – весовой коэффициент инцидента.

Детектор фиксирует факт принудительного прерывания сессии и генерирует инцидент типа «Разрыв сессии».

5.4 Контроль привычного времени работы

Рассматриваемый детектор фиксирует действия, которые обнаруживаются при активности персоны в нехарактерный для нее период времени работы.

Это может быть признаком злоупотребления целевой учетной записью, попыток кражи данных или какого-либо сбоя в инфраструктуре, требующего принятия срочных мер со стороны администратора.

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – количество дней, в течение которых происходит накопление необходимой статистики зафиксированных фактов какой-либо активности со стороны пользователя в периоды времени, которые выходят за рамки установленного окна времени (3);
- (3) – ширина окна времени, которое является корректирующим значением, выход за которое не является признаком аномального поведения;
- (4) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (5) – весовой коэффициент инцидента.

Активировать

Уровень
Низкий (1)

Дни до учета
60 (2)

Ширина временного окна в минутах
60 (3)

Группы
* (4)

Коэффициент
1.0 (5)

Сохранить

При выходе за пределы стандартных диапазонов работы генерируется инцидент типа «Необычное время работы».



Настройку диапазонов значений по количеству сессий и размеру окна времени нежелательно часто корректировать. После изменения этих настроек потребуется некоторое время по накоплению новой статистики для нормальной работы.

5.5 Контроль изменения уровня доверия

За каждой персоной закреплён количественный показатель **Уровня доверия**, который представляет собой профиль поведения рассматриваемой **Персоны**, формирующийся с учетом накопленной статистики ее аномального поведения. Анализируются одновременно в разрезе дня и сессии различные активности **Персоны**. Отслеживаются три активности:

- количество подключений (только в разрезе дня);
- количество событий;
- объем загруженных или выгруженных данных.

При генерировании инцидента, источником которого является рассматриваемая персона, значение **Уровня доверия** уменьшается в зависимости от следующих показателей срабатываемых детекторов аномалий:

- Коэффициент влияния
- Уровень критичности

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

Активировать

Низкий уровень

Порог
450 (2)

Уровень
Низкий (1) ▼

Коэффициент
1,0 (6)

Средний уровень

Порог
300 (3)

Уровень
Средний (1) ▼

Коэффициент
1,0 (6)

Высокий уровень

Порог
200 (4)

Уровень
Высокий (1) ▼

Коэффициент
1,0 (6)

Критический уровень

Порог
1 (5)

Уровень
Критичный (1) ▼

Коэффициент
1,0 (6)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – порог низкого уровня доверия;
- (3) – порог среднего уровня доверия;
- (4) – порог высокого уровня доверия;
- (5) – порог критического уровня доверия;
- (6) – весовой коэффициент инцидента.

Если текущий уровень доверия персоны опускается ниже настраиваемых пороговых значений, то генерируется инцидент типа «Уровень доверия». Уровень генерируемого инцидента зависит от того, ниже какого порога опустилось значение **Уровня доверия**.



Рисунок 8 – Уровни доверия

5.6 Контроль стандартных команд

Детектор анализирует команды в максимально абстрактном виде, в результате чего строится базовое поведение **Персоны**. При обоснованном подозрении, что наблюдается серьезное отклонение от ранее зафиксированного потока команд, который система выучила за настроенный период, детектор создает инцидент.

Активировать

Уровень
Низкий (1)

Группы
* (2)

Коэффициент
1.0 (3)

Максимальный процент разницы
50 (4)

Укороченный
Глубина истории в днях
30 (5)

Настроенный
Авто (6)

Работает, если настроено вручную
Значение новой длины, в процентах
10 (7)

Важность новых команд, процент
50 (8)

Важность перестановки команд, проценты
40 (9)

Масштабирование
0 (10)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – Уровень критичности инцидента;
- (2) – Перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (3) – Весовой коэффициент инцидента;
- (4) – Процент отличия, начиная с которого сессия считается подозрительной;

- (5) – Число календарных дней, которые учитываются для анализа. При отсутствии галочки учитываются все сессии пользователя;
- (6) – Параметр, который показывает, выбраны ли рекомендуемые настройки наших разработчиков (**АВТО**), либо простые и прозрачные параметры подбирает офицер безопасности (**СОЗДАН ВРУЧНУЮ**). Параметры, выбираемые вручную, в сумме должны давать 100%, иначе будет автоматическое масштабирование чисел пропорционально введенным значениям.
- (7) – Количественная реакция на нетипичное количество команд в сессии. Если этот параметр ненулевой, то сессия с нетипичным количеством команд для персоны получит указанное значение процентов в отличие от предыдущих сессий;
- (8) – Количественная реакция на нетипичные для персоны команды в сессии;
- (9) – Количественная реакция на нетипичные для персоны последовательности команд глубиной до пяти;
- (10) – Параметр, принимающий значения 0 (не применяется) или 1 (применяется). Показывает, будет ли происходить перераспределение процентов важности для перестановки команд для коротких сессий.

Необычные вызовы команд в сценариях регулярного обслуживания могут указывать на случаи неисправности или на то, что кто-то совершает подозрительные действия.

Детектор создает инцидент типа «Необычные команды».

5.7 Контроль привычных сетевых адресов

Рассматриваемый детектор будет использовать базовые данные об активности из профиля **Персоны** и будет реагировать, если **Персона** попытается подключиться из неизвестного сетевого местоположения. Попытки получить удаленный доступ из неизвестных сетевых местоположений могут представлять риск взлома учетных записей или эпидемий вредоносных программ.

После обнаружения нового адреса источника этот механизм добавляет обнаруженную подсеть адреса источника в профиль **Персоны** для сбора информации об адресе источника для будущего использования.

Активировать

Уровень

Низкий (1)

Группы

* (2)

Коэффициент

1.0 (3)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;

(3) – весовой коэффициент инцидента.

В ситуациях, когда персона предпринимает попытку доступа к целевой системе из другой подсети, детектор создает инцидент типа «Сетевое расположение».

5.8 Контроль эффективности работы

Детектор оценивает время сессии исходя из накопленной информации для конкретной персоны и сигнализирует о его резком изменении (падении или значительном превышении). Собранные данные агрегируются в отчете по эффективности сессии.

Активировать

Уровень
Низкий (1) ▾

Период
60 (2)

Минимальное влияние инцидентов
40 (3)

Группы
* (4) ▾

Коэффициент
1.0 (5)

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – период (указывается в количестве дней) – это количество дней, в течение которых фиксируется активность персон;



Допустимый уровень активности, при превышении которого начинает работать рассматриваемый детектор, рассчитывается с учетом статистики активности, зафиксированной за последнее количество дней, которое указывается в (2).

- (3) – степень влияния инцидента;
- (4) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (5) – весовой коэффициент инцидента.

Низкие значения коэффициента могут означать проблемы с организацией рабочих процессов.

5.9 Индикаторы взрывной активности

Рассматриваемый детектор реагирует на необычный уровень активности **Персоны**, используя собранную информацию из её предыдущих сессий. В качестве активности независимо рассматриваются количество сессий за день, количество событий внутри сессий и объем

передаваемых или получаемых файлов. Производится сравнение для рассматриваемой **Персоны** долгосрочного среднего значения активности с текущей активностью, и при значительных превышениях активности создается инцидент.

Такие изменения уровня активности могут быть признаком взлома целевых учетных записей или некоторых особенностей инфраструктуры, требующих принятия срочных мер со стороны администратора для их устранения.

Под активностью персоны следует понимать:

- количество сессий подключения к целевой системе;
- количество событий в течение сессии подключения к целевой системе;
- объем передаваемых файлов в рамках сессии подключения к целевой системе.

Активировать

Уровень
Низкий (1)

Период
32 (2)

Группы
* (3)

Коэффициент
1.0 (4)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – период (указывается в количестве дней) – это количество дней, в течение которых фиксируется активность персон;



Допустимый уровень активности, при превышении которого начинает работать рассматриваемый детектор, рассчитывается с учетом статистики активности, зафиксированной за последнее количество дней, которое указывается в (2).

- (3) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (4) – весовой коэффициент инцидента.

Данный детектор генерирует инцидент типа «Индикаторы взрывной активности», когда активность пользователя превышает его среднюю активность за рассматриваемый период времени.

5.10 Детектор новых доступов

На основе существующих исходных данных о конкретной **Персоне** рассматриваемый детектор информирует офицеров службы безопасности о том, что право доступа используется впервые. Если **Персона** достаточно долго отслеживается в системе (настройка в аномалиях есть как "дни до учета",

число дней должно быть больше указанного), то детектор определяет, не использует ли персона новый аккаунт или сервис на "знакомой" целевой системе, не новая ли целевая система.

Если таких событий много, это может быть признаком опасной ситуации:

- Массовый сбой, требующий интенсивного использования Шлюза доступа.
- Ошибка политики доступа, предоставляющая **Персоне** дополнительные права доступа.
- Попытки сбора и кражи данных.
- Взломанная целевая учетная запись администратора.

Активировать

Уровень
Низкий (1)

Дни до учета
7 (2)

Группы
* (3)

Коэффициент
0.1 (4)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – количество дней, пока учет данных не ведется;
- (3) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (4) – весовой коэффициент инцидента.

Данный детектор генерирует инцидент типа «Новый доступ», когда пользователь осуществляет доступ к учетной записи или целевой системе, к которым ранее доступ отсутствовал.

5.11 Детектор проблем с правами доступа к файлам

Рассматриваемый детектор отслеживает сеансы передачи файлов по протоколу SFTP. В случае попыток доступа к файлам или каталогам с недостаточными правами детектор будет создавать инциденты. Эти инциденты могут быть признаком кражи информации, компрометации целевой учетной записи или ошибок настройки прав доступа.

Активировать

Уровень
Низкий (1)

Группы
* (2)

Коэффициент
1.0 (3)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (3) – весовой коэффициент инцидента.

В случае обнаружения ошибок доступа на осуществление операций чтения или записи (Permission denied) детектор генерирует инцидент типа «Недостаток прав».

5.12 Детектор туннелей и прыжков

Обнаруживает случаи, когда отслеживаемая **Персона** выполняет команды или другие действия с целью открытия дополнительных сетевых каналов до инфраструктуры в рамках рассматриваемой пользовательской сессии целевой системы:

- дополнительные туннели SSH к определенным адресам и портам;
- запуск команд удаленного доступа в рамках сессий удаленного доступа (SCP, SSH и др.)

Такие случаи можно рассматривать как признак того, что целевая учетная запись администратора была взломана или были предприняты попытки собрать информацию о защищенной инфраструктуре.

Список агентов для организации удаленного доступа может быть сформирован при настройке рассматриваемого детектора аномалий.

Активировать

Уровень: Средний (1)

Агенты: ssh, mstsc, vnc, rdesktop, scp (2)

Включая localhost

Группы: * (3)

Коэффициент: 1.0 (4)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – перечень имен сервисов;
- (3) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (4) – весовой коэффициент инцидента.

При необходимости ставится флаг для учета переходов по localhost.

В случае обнаружения признаков использования указанных в (2) сервисов генерируется инцидент типа «Туннели и прыжки».

5.13 Детектор входов помимо бастиона

Рассматриваемый детектор позволяет сигнализировать о доступе к целевым системам на основании данных, получаемых от анализаторов сетевых потоков третьих производителей, таких как KICS (производства Kaspersky), PT ISIM (производства Positive Technologies) и др.

Детектор срабатывает при обнаружении удаленного доступа к целевой системе, который осуществляется в обход Шлюзов доступа.

Такой случай может сигнализировать о нарушении политики доступа к критически важным ресурсам инфраструктуры.

Активировать

Уровень

Высокий (1)

Группы

* (2)

Коэффициент

1.0 (3)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (3) – весовой коэффициент инцидента.

В результате срабатывания рассматриваемого детектора генерируется инцидент «Прямой доступ».

5.14 Анализатор ошибок авторизации

Рассматриваемый детектор создает инциденты, которые являются результатом реакции на ошибки авторизации во время попыток подключения к целевым системам.

Причинами возникновения ошибок авторизации могут быть:

- атаки методом грубой силы;
- ошибки прав доступа;
- активности вредоносного ПО;
- вторжения.

Уровень критичности созданных инцидентов будет повышаться в случае, если за последнее время было зафиксировано большое количество случаев сбоя аутентификации с определенного адреса источника или от рассматриваемой **Персоны**.

Активировать

Уровень

Низкий (1)

Группы

* (2)

Коэффициент

0.1 (3)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (3) – весовой коэффициент инцидента.

В результате срабатывания рассматриваемого детектора генерируется инцидент «Ошибка аутентификации».

5.15 Детектор забытых персон

Рассматриваемый детектор позволяет фиксировать доступ **Персоны** к целевой системе после продолжительного периода времени отсутствия какого-либо доступа **Персоны** к целевой системе. Если в системе долгое время не было данных об активности **Персоны**, а затем регистрируется новый сеанс, то будет создан инцидент.

Инциденты такого рода могут указывать на риски взлома целевых учетных записей или попытки злоумышленника собрать информацию об инфраструктуре.



В зависимости от периода отсутствия доступа к целевой системе определяются три уровня критичности инцидента, для которых задаются индивидуальные весовые коэффициенты.

Активировать

Группы
- (1)

Уровень
Низкий (2)

Коэффициент
1.0 (3)

Дней отсутствия от
91 (4)

Уровень
Средний (2)

Коэффициент
1.0 (3)

Дней отсутствия от
182 (4)

Уровень
Высокий (2)

Коэффициент
1.0 (3)

Дней отсутствия от
365 (4)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (2) – уровень критичности инцидента (для каждого указанного временного промежутка);
- (3) – весовой коэффициент инцидента (для каждого указанного временного промежутка);
- (4) – количество дней отсутствия доступа персоны к целевой системе (для каждого указанного временного промежутка).

В результате срабатывания рассматриваемого детектора генерируется инцидент «Забытая персона».

5.16 Количество переданных файлов

Рассматриваемый детектор позволяет контролировать количество переданных файлов в течение пользовательской сессии целевой системы. Регулярная передача тысяч файлов создает серьезную нагрузку на инфраструктуру и может занять много времени из-за неэффективных процессов.

Массовая передача файлов может быть признаком кражи информации или активности вредоносного ПО.

Активировать

Уровень
Низкий (1)

Низкий уровень нагрузки
2000 (2)

Средний уровень нагрузки
10000 (3)

Высокий уровень нагрузки
30000 (4)

Период
32 (5)

Группы
* (6)

Коэффициент
1.0 (7)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – количество переданных файлов для закрепления низкого уровня нагрузки;
- (3) – количество переданных файлов для закрепления среднего уровня нагрузки;
- (4) – количество переданных файлов для закрепления высокого уровня нагрузки;
- (5) – период (указывается в количестве дней) – за указанное количество дней рассчитывается среднее количество переданных персонами файлов в течение сессий доступа к целевым системам;
- (6) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (7) – весовой коэффициент инцидента.

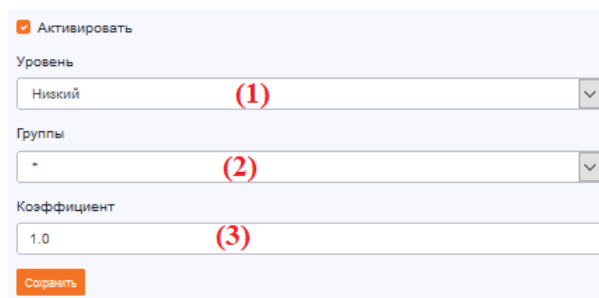
В результате срабатывания рассматриваемого детектора генерируется инцидент «Количество переданных файлов».



В зависимости от указанного уровня нагрузки (среднего количества переданных файлов) генерируемый инцидент имеет соответствующий уровень критичности.

5.17 Детектор сканеров

Рассматриваемый детектор позволяет фиксировать множественные попытки доступа без дальнейшей авторизации к целевой системе от конкретного источника в течение короткого времени.



Активировать

Уровень
Низкий (1)

Группы
- (2)

Коэффициент
1.0 (3)

Сохранить

Для рассматриваемого детектора администратору необходимо настроить следующие параметры:

- (1) – уровень критичности инцидента;
- (2) – перечень групп персон, пользовательские сессии которых будут подвергаться анализу рассматриваемым детектором;
- (3) – весовой коэффициент инцидента.

В результате срабатывания рассматриваемого детектора генерируется инцидент «Сканеры».

6 НАСТРОЙКА ИСТОЧНИКОВ ПОЛЬЗОВАТЕЛЬСКИХ СЕССИЙ ЦЕЛЕВЫХ СИСТЕМ

Источником данных для СКДПУ НТ может быть:

- Шлюз Доступа (СКДПУ);
- файлы, содержащие набор различных событий;
- системы сторонних производителей.

Параметры передачи данных событий пользовательских сессий целевых систем указаны в файле конфигурации `/opt/skdpu-nt/etc/syslog-ng.conf`.

6.1 Шлюз доступа

Для получения данных от СКДПУ необходимо в разделе веб-интерфейса СКДПУ **Интеграция с SIEM** настроить отправку событий в СКДПУ НТ (см. [рисунок 9](#)).



Для СКДПУ версии 5 рекомендуется использовать порт 514/tcp. Для СКДПУ версии 7 и выше рекомендуется использовать порт 515/tcp.

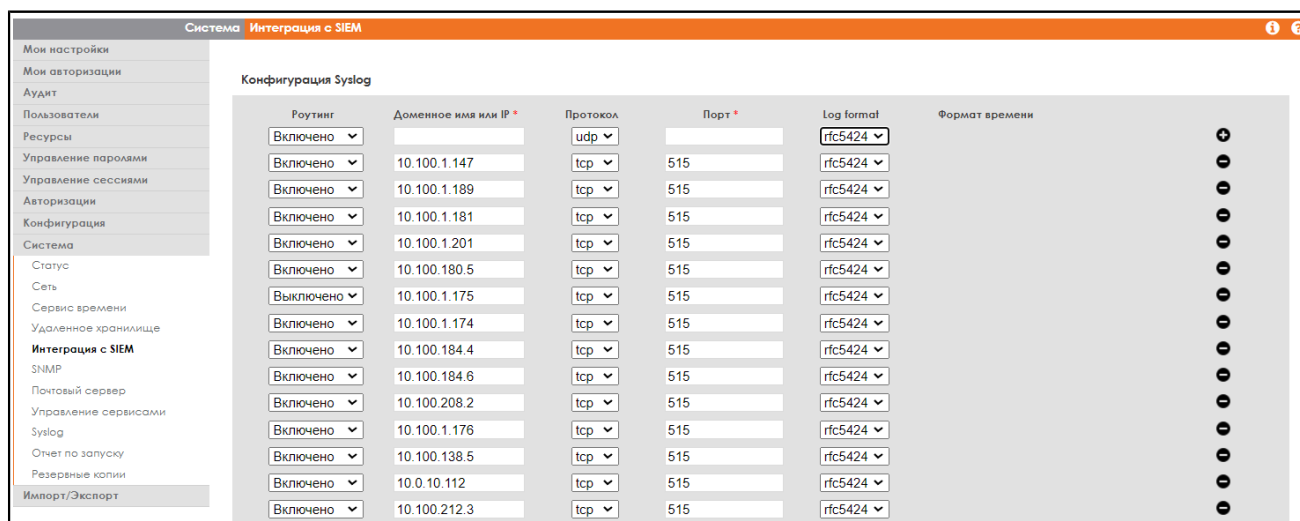


Рисунок 9 – Настройка интеграции с SIEM

Для получения большей части данных, включая нажатия клавиш и данные буфера обмена, необходимо включить флаг **Сложные настройки** в правом верхнем углу экрана и установить следующие параметры в разделе веб-интерфейса СКДПУ **Конфигурация>Настройки>RDP Proxy**:

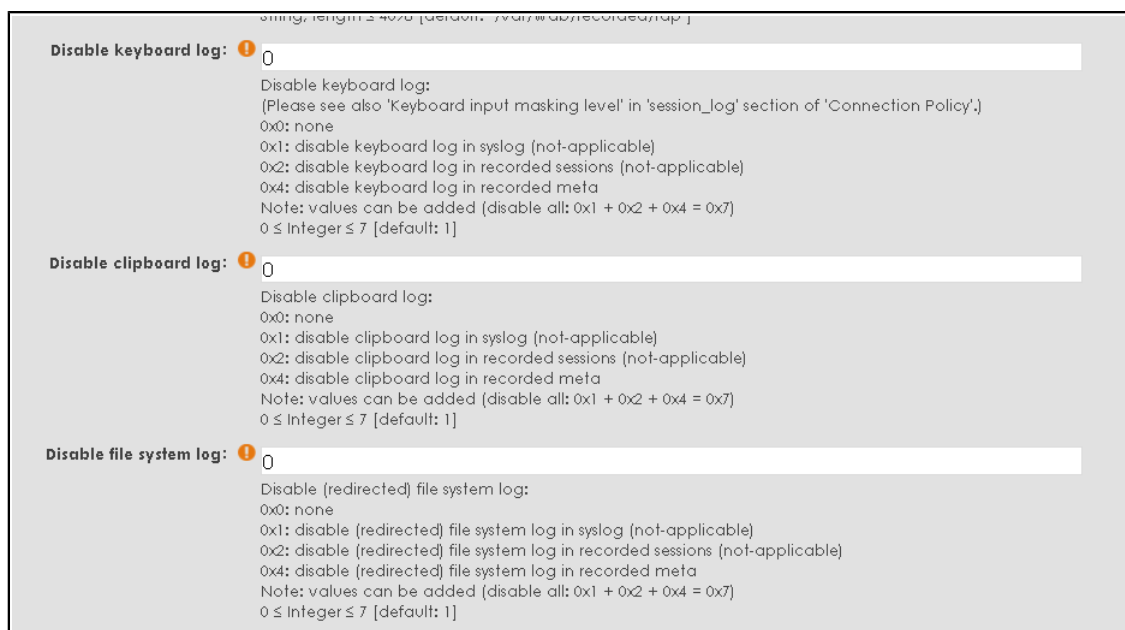


Рисунок 10 – СКДПУ версии 7

При правильной настройке в разделе веб-интерфейса СКДПУ NT **Сессии** должны отобразиться пользовательские сессии с целевых систем, произведенные после настройки СКДПУ.

6.2 Файл с событиями

В СКДПУ NT события пользовательских сессий на целевых системах можно передавать из файла с соответствующими событиями, для этого необходимо использовать следующую команду:

```
cat log.txt | /opt/skdpu-nt/bin/collect -v
```

log.txt - файл с событиями.

В СКДПУ NT события пользовательских сессий на целевых системах можно передать посредством файлов, содержащих перечень событий пользовательских сессий.

Например, перечень файлов пользовательских сессий содержится в архиве `test-set-v0.1.tgz`:

Шаг 1. Перенести архив `test-set-v0.1.tgz` в директорию `/home/ntadmin`.

Шаг 2. Получить права суперпользователя.

Шаг 3. Перейти в директорию `/home/ntadmin` и распаковать архив

```
cd /home/ntadmin
tar -zxvf test-set-v0.1.tgz
```

Шаг 4. Перейти в директорию `test-set` и запустить выгрузку набора пользовательских сессий

```
cd /test-set
for i in *.log; do echo $i; cat $i | /opt/skdpu-nt/bin/rewrite
| /opt/skdpu-nt/bin/collect -v; done
```

Шаг 5. Дождаться окончания переноса сессий.

6.3 Системы сторонних производителей

Данные о попытках доступа к целевым ресурсам также можно получать от систем сторонних производителей. Источником таких данных для СКДПУ НТ являются файлы с расширением `*.sock`, расположенные в директории `/opt/skdpu-nt-data/log/`, или по интерфейсу API.

Настройка подключения к PT ISIM

Настройка отправления событий в СКДПУ НТ осуществляется через консоль посредством внесения изменения в конфигурационные файлы на сервере, где установлен PT ISIM.

- Шаг 1. Получить доступ к серверу, где установлен PT ISIM, по SSH.
- Шаг 2. Получить права суперпользователя.
- Шаг 3. Настроить формат событий, создав файл `/var/mapping.conf` со следующим содержанием

```
time = [time]
Network.IPv4.src_addr = [Network.IPv4.src_addr]
Network.IPv4.dst_addr = [Network.IPv4.dst_addr]
src.port = [Network.IPv4.TCPv4.src_port,
  Network.IPv4.UDPv4.src_port, Network.IPv4.ICMPv4.src_port]
dst.port = [Network.IPv4.TCPv4.dst_port,
  Network.IPv4.UDPv4.dst_port, Network.IPv4.ICMPv4.dst_port]
protocol = [Protocol.protocol]
event_type = [Event.event_type]
dst.mac = [Physical_Medium.Ethernet.dst_mac]
src.mac = [Physical_Medium.Ethernet.src_mac]
Event.proto_family = [Event_proto_family]
```

- Шаг 4. В поле `config` блока `siem` файла `/opt/ptisim/etc/ptisim.conf` указать путь к файлу `/var/mapping.conf` и в блоке `features` установить значение параметра `siem` в значение `true`

```
"siem": {
  "config": "/var/mapping.conf",
  "mode": "json"
},
...
"features": {
  "splitter": true,
  "nsolver": true,
  "tsolver": false,
  "table_scheme_validation": false,
  "siem": true,
  "test": {
    "splitter": false,
    "normalization": false,
    "routing": false,
    "correlation": false,
    "http": false
  }
}
```

Шаг 5. В файле `/etc/rsyslog.conf` определить требуемый формат сообщений `syslog` и указать IP-адрес сервера СКДПУ НТ `<ip_nt>`, куда будут отправляться сообщения

```
template(name="rfc5424" type="list") {
    constant(value("<")
    property(name="pri")
    constant(value(">1 ")
    property(name="timestamp" dateFormat="rfc3339"
date.inUTC="on")
    constant(value=" ")
    property(name="hostname" position.from="1" position.to="255"
caseConversion="lower")
    constant(value=" ")
    property(name="programname" position.from="1" position.to="48"
caseConversion="lower")
    constant(value=" ")
    property(name="procid" position.from="1" position.to="128")
    constant(value=" ")
    property(name="msgid" position.from="1" position.to="32")
    constant(value=" ")
    property(name="structured-data")
    constant(value=" ")
    property(name="msg" droplastlf="on")
    constant(value="\n")
}

if ($syslogtag == 'ISIM:') then {
    action (type="omfwd" TCP_Framing="octet-counted"
Target="<ip_nt>" Port="516" Protocol="tcp" template="rfc5424")
    stop
}
```



Необходимо удостовериться, что для порта 516 в файле `/opt/ptisim/etc/secure-iptables.rules` добавлено правило

```
-A OUTPUT -p tcp --dport 516 -m state --state NEW,ESTABLISHED -j
ACCEPT
```

На сервере СКДПУ НТ в файл `/opt/skdpu-nt/etc/engines.json` необходимо добавить подключение к файлу `opt/skdpu-nt/data/log/isim.sock`

```
{
  "id" : 2,
  "kind": "IsimEngine",
  "version": 1,
  "active": true,
  "source": "/opt/skdpu-nt/data/log/isim.sock"
}
```

Перезапустить сервис `enrichd`

```
systemctl restart enrichd.service
```

Настройка подключения к KICS

Настройка отправления событий в СКДПУ НТ осуществляется через веб-интерфейс KICS.

Шаг 1. В строке веб-браузера ввести IP-адрес сервера KICS.

Шаг 2. Авторизоваться в веб-интерфейсе KICS.

Шаг 3. Добавить коннектор для подключения к СКДПУ НТ, заполнив соответствующие поля

The screenshot shows the 'Создание коннектора' (Create Connector) dialog box in the KICS interface. The dialog is overlaid on a table of existing connectors. The 'Create Connector' form has several fields highlighted with red boxes:

- Имя пользователя:** Kics
- Адрес сервера:** Адрес сервера KICS for Net
- Адрес узла коннектора:** Адрес сервера СКДПУ НТ
- Пароль доступа к сертификату коннектора:** Пароли на сертификат
- Имя коннектора:** Имя коннектора в интерфейсе
- Тип коннектора:** Для REST API -- Generic
- Отправляемые сообщения программы:** Все
- Отправляемые записи аудита:** Все

A 'Сохранить' (Save) button is also highlighted at the bottom of the dialog.

Шаг 4. Сохранить коннектор (например, коннектор_skdpu-nt-api.zip).

Шаг 5. Распаковать архив коннектор_skdpu-nt-api.zip и перенести файлы certificates.pfx и metadata.json на сервер СКДПУ НТ в директорию /home/ntadmin/api/.

Продолжить настройку на сервере СКДПУ НТ:

Шаг 1. В консоли ОС сервера, где установлен СКДПУ НТ, войти в режим суперпользователя.

Шаг 2. Перейти в директорию /home/ntadmin/api/

Шаг 3. Сгенерировать сертификат connector.crt с последующим вводом пароля на сертификат certificates.pfx

```
root@skdpu-nt:/home/ntadmin/api# openssl pkcs12 -in
  certificates.pfx -clcerts -nokeys -out connector.crt
Enter Import Password:
```

- Шаг 4. Сгенерировать ключ `connector.key` с последующим вводом пароля на сертификат `certificates.pfx`

```
root@skdpu-nt:/home/ntadmin/api# openssl pkcs12 -in
certificates.pfx -nocerts -out connector.key
Enter Import Password:
```

- Шаг 5. Задать пасс-фразу для ключа

```
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

- Шаг 6. Записать ключ RSA

```
root@skdpu-nt:/home/ntadmin/api# openssl rsa -in connector.key -
out connector.key
Enter pass phrase for connector.key:
writing RSA key
```

- Шаг 7. Переместить созданные ключи в директорию `/opt/skdpu-nt/var/ssl`

```
root@skdpu-nt:/home/ntadmin/api# mv connector.crt connector.key
```

- Шаг 8. В файл `/opt/skdpu-nt/etc/engines.json` необходимо добавить подключение к файлу `opt/skdpu-nt/data/log/kics.sock`

```
{
  "id": 3,
  "kind": "KicsEngine",
  "version": 2,
  "active": true,
  "ports": [ 22, 23, 3389, 5900 ],
  "source": {
    "type": "syslog",
    "path": "/opt/skdpu-nt-data/log/kics.sock"
  },
  "transport": "rmq"
}
```

и подключение по API к серверу `<ip_KICS>` с помощью сгенерированных ранее сертификата `connector.crt` и ключа `connector.key`

```
{
  "id": 4,
  "kind": "KicsEngine",
  "version": 2,
  "active": false,
  "ports": [ 22, 23, 3389, 5900 ],
  "source": {
    "type": "api",
    "cert": "/opt/skdpu-nt/var/ssl/connector.crt",
    "key": "/opt/skdpu-nt/var/ssl/connector.key",
    "uri": "https://<ip_KICS>/kics/api",
    "poll_interval": 10
  },
  "transport": "rmq"
}
```

Шаг 9. Перезапустить сервис enrichd

```
systemctl restart enrichd.service
```

7 НАСТРОЙКА

7.1 Общие сведения

В разделе **Настройки** представлены функциональные возможности, которые позволяют администратору СКДПУ НТ редактировать информацию о настройках компонентов как СКДПУ НТ, так и компонентов среды функционирования, управлять парольной политикой СКДПУ НТ, осуществлять управление системными журналами и журналами аудита СКДПУ НТ.

В раздел входят следующие подразделы:

- **Основные настройки;**
- **Системные настройки;**
- **Настройки LDAP;**
- **Конфигурация журналирования;**
- **Информация о лицензии.**

Осуществлять поиск по записям можно через элемент **Поиск**. После ввода двух и более символов отображаемые сервисы будут отсортированы в соответствии с введенными данными.

7.2 Основные настройки

В рассматриваемом разделе администратор СКДПУ НТ имеет возможность править в настройке соединения с почтовым сервером, осуществлять настройки веб-интерфейса СКДПУ НТ, а также управлять системой отчетов, которые генерируются в процессе выявления инцидентов.

Система не имеет средств внесения изменений в журналы функционирования, но позволяет настроить их расположение, при необходимости.

Наиболее подробный уровень отладочной информации «4».

7.2.1 Настройка параметров соединения с почтовым сервером

Для настройки параметров подключения почтового сервера необходимо:

Шаг 1. В разделе **Настройки**>**Основные настройки** нажать  .

Шаг 2. Далее раскрыть элемент **Почтовый сервер** нажатием левой кнопки мыши

Почтовый сервер

Протокол: SMTP + STARTTLS (1)

Имя пользователя: mailbot@it-bastion.com (4)

Адрес сервера: smtp.yandex.com (2)

Пароль: Пароль установлен (5)

Порт: 465 (3)

Подтверждение пароля: (6)

Очистить реквизиты

Имя отправителя: SKDPU NT 181 (7)

Почтовый адрес отправителя: mailbot@it-bastion.com (8)

Сохранить

Шаг 3. Внести необходимые настройки в соответствующие поля:

- (1) – протокол передачи сообщений (SMTP, SMTPS, SMTP+STARTTLS);
- (2) – адрес почтового сервера;
- (3) – порт почтового сервера;
- (4) – имя пользователя почтового сервера;
- (5) – пароль для авторизации на почтовом сервере;
- (6) – подтверждение пароля;
- (7) – имя отправителя, которое указывается в письме с отчетом;
- (8) – почтовый адрес отправителя.

Шаг 4. Чтобы зафиксировать внесенные изменения необходимо нажать **Сохранить**.

При успешном сохранении настроек появится оповещение

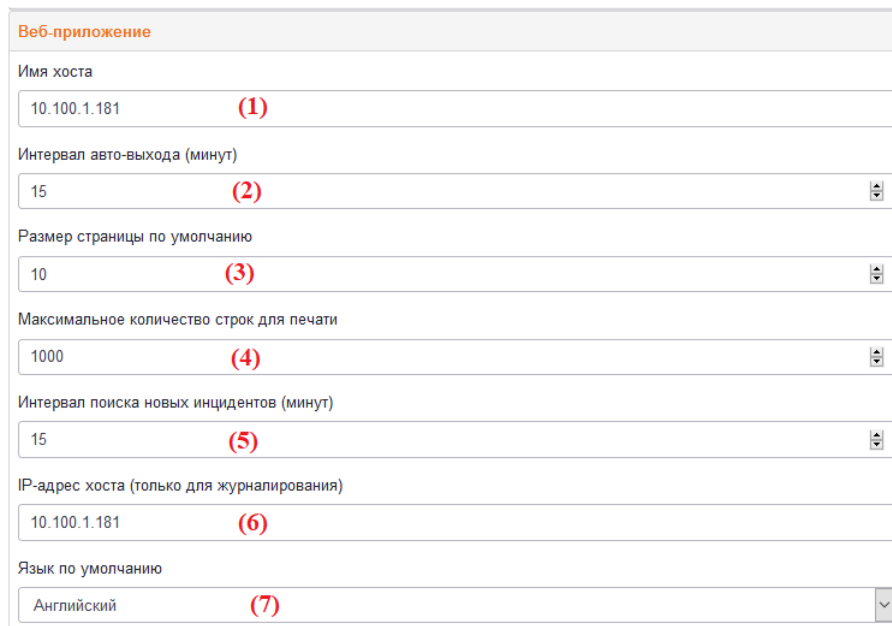
Конфигурация успешно обновлена

7.2.2 Настройка веб-интерфейса

Для настройки параметров веб-интерфейса необходимо:

Шаг 1. В разделе **Настройки>Основные настройки** нажать **Редактировать**.


Шаг 2. Далее раскрыть элемент **Веб-приложение** нажатием левой кнопки мыши



Веб-приложение	
Имя хоста	10.100.1.181 (1)
Интервал авто-выхода (минут)	15 (2)
Размер страницы по умолчанию	10 (3)
Максимальное количество строк для печати	1000 (4)
Интервал поиска новых инцидентов (минут)	15 (5)
IP-адрес хоста (только для журналирования)	10.100.1.181 (6)
Язык по умолчанию	Английский (7)

Шаг 3. Внести необходимые настройки в соответствующие поля:

(1) – имя хоста;

 Указывается в поле *dvchost* при регистрации событий в СКДПУ НТ.


(2) – время бездействия, после которого происходит прерывание сессии доступа к веб-интерфейсу;

(3) – количество строк на одной странице таблицы в интерфейсе;

(4) – максимальное количество строк при печати отчетов;

(5) – интервал поиска новых инцидентов (указывается в минутах);

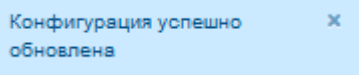
(6) – IP-адрес хоста;

 Указывается в поле *dst* при регистрации событий в СКДПУ НТ.

(7) – язык страницы авторизации веб-интерфейса.

Шаг 4. Чтобы зафиксировать внесенные изменения необходимо нажать  .

При успешном сохранении настроек появится оповещение



Конфигурация успешно обновлена

7.2.3 Управление системой отчетов

Для настройки системы отчетов необходимо:

Шаг 1. В разделе **Настройки>Основные настройки** нажать  .

Шаг 2. Далее раскрыть элемент **Отчеты** нажатием левой кнопки мыши

Отчеты

Время хранения (месяцев)

1 (1)

Максимальное количество строк

2000 (2)

Максимальное количество строк для предпросмотра

50 (3)

Сохранить

В рассматриваемой форме для изменения доступны следующие настройки системы отчетов:

- (1) – время хранения отчетов (указывается в месяцах);
- (2) – максимальная количество строк в отчете;
- (3) – максимальное количество строк в отчете для предпросмотра.

Шаг 3. Внести необходимые настройки в соответствующие поля.

Шаг 4. Чтобы зафиксировать внесенные изменения необходимо нажать **Сохранить**.

При успешном сохранении настроек появится оповещение

Конфигурация успешно обновлена

7.3 Системные настройки

Данные настройки относятся к базовым настройкам системы.

i Рекомендуется без необходимости не изменять их значение

Тайм-аут сессии (GC) - максимальная продолжительность пользовательских сессий целевых систем в часах.

i Если у пользовательской сессии целевой системы отсутствует отметка о закрытии и ее продолжительность превышает данный показатель, то ей присваивается отметка о закрытии

Записей уровня доверия на человека - количество последних значений уровня доверия персон, которые учитываются в статистике изменения.

i Если количество значений уровня доверия превышает данный показатель, то более ранние записи удаляются

В СКДПУ НТ выполняется регулярная очистка, чтобы поддерживать архив данных в актуальном состоянии. Старые записи являются предметом процесса ротации данных. Для

автоматического удаления старых данных СКДПУ НТ настраивается в соответствии с принятыми в эксплуатирующей организации руководящими документами по хранению и защите данных.

По умолчанию применяются следующие настройки хранения данных:

- **Держать Инциденты в течение (месяцев)** - время до того, как старые записи об инцидентах будут удалены из архива. Значение по умолчанию - 6 месяцев
- **Хранить сессии в архиве (месяцы)** - время до того, как старые записи сессии будут удалены из архива. Значение по умолчанию - 8 месяцев
- **Сохранять цели после последнего сеанса (месяцы)** - время бездействия до того, как профили целей будут удалены из архива. Значение по умолчанию - 12 месяцев
- **Держать людей после последнего сеанса (месяцев)** - время бездействия до того, как профиль пользователя будет удален из архива. Значение по умолчанию - 18 месяцев
- **Хранить данные промежуточного анализа в течение (месяцев)** - хранит набор внутренних наборов данных для профилирования действий пользователя. Эти записи будут храниться не более установленного временного окна. Значение по умолчанию - 6 месяцев
- **Хранить архивы экспорта в течение (месяцев)** - перед тем, как сессии будут полностью удалены, записи помещаются в архивы во время регулярной задачи сохранения данных. Эти архивы хранятся в течение нескольких месяцев. Значение по умолчанию - 3 месяца

7.4 Настройки LDAP

В данном разделе администратор СКДПУ НТ имеет возможность редактировать подключения к доменам и серверам LDAP в целях обеспечения аутентификации пользователей СКДПУ НТ по протоколу LDAP (см. [рисунок 11](#)).

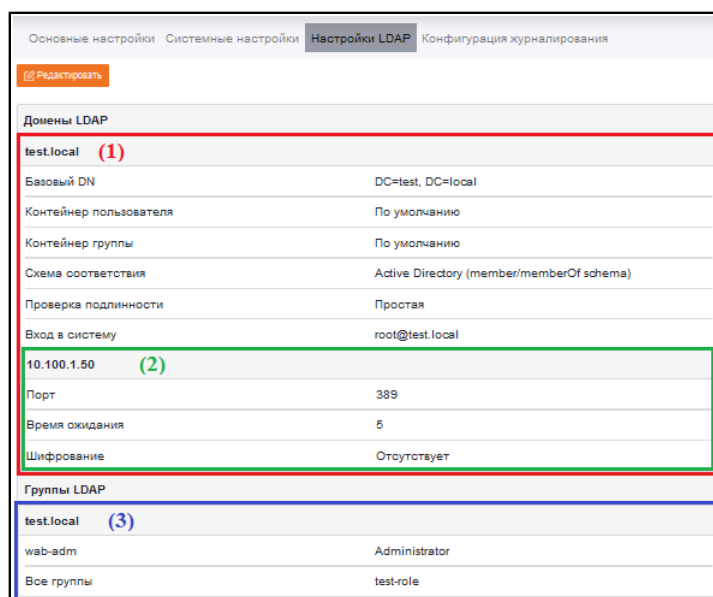


Рисунок 11 – Раздел Настройки > Настройки LDAP

(1) – домен LDAP;

(2) – сервер, где развёрнута служба каталогов LDAP;

- (3) – группы LDAP, определенные в структуре домена LDAP, и ассоциированные с ними роли пользователей СКДПУ НТ.



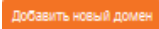
LDAP-пользователь не существует в системе до тех пор, пока с его учётными данными не был осуществлён вход. Наличие пользователя в домене LDAP не означает, что администратор может осуществлять с ним какие-то действия.

7.4.1 Домен LDAP

7.4.1.1 Добавление нового домена LDAP

Для добавления нового домена LDAP необходимо:

Шаг 1. В разделе **Настройки**>**Настройки LDAP** нажать .

Шаг 2. В появившейся форме нажать .

Шаг 3. Заполнить необходимые поля и добавить в домен как минимум один сервер LDAP (см. раздел 7.4.2.1)

Новый домен

Имя (1)

По умолчанию

Базовый DN (2)

Контейнер пользователя (3)

Computer container (4)

Контейнер группы (5)

Схема соответствия (6)

Проверка подлинности (7)

Вход в систему

Пароль

В рассматриваемой форме доступны для изменения следующие настройки LDAP сервера:

- (1) – имя (идентификатор) сервера;
- (2) – базовый DN (уникальное имя);
- (3) – контейнер пользователя;
- (4) – контейнер компьютера;
- (5) – контейнер группы;
- (6) – схема соответствия:
 - Active Directory (member/memberOf schema);
 - Active Directory (member/memberOf schema), no group hierarchy;
 - LDAP (member-uniqueMember schema);
 - POSIX (gidNumber/memberUid schema).
- (7) – проверка подлинности:
 - простая;
 - NTLM;
 - SASL;



В СКДПУ HT поддерживаются следующие механизмы аутентификации SASL:

- внешняя;
 - дайджест MD5;
 - Kerberos;
 - логин/пароль.
- анонимный доступ.



В зависимости от выбранного типа проверки подлинности необходимо будет заполнить дополнительные поля.

Шаг 4. Сохранить настройки [Сохранить](#).

При успешном сохранении настроек появится оповещение

Конфигурация успешно обновлена

7.4.1.2 Удаление домена LDAP

Для удаления домена LDAP необходимо:

Шаг 1. В разделе **Настройки**>**Настройки LDAP** нажать [Редактировать](#).

Шаг 2. В появившейся форме выбрать соответствующий домен LDAP и нажать [Удалить домен](#).

The screenshot shows a configuration form for a domain named 'test_domain'. The form includes the following fields and controls:

- Имя:** test_domain
- По умолчанию:** [Установить](#)
- Базовый DN:** DC=test, DC=local
- Контейнер пользователя:** (empty text field)
- Контейнер группы:** (empty text field)
- Схема соответствия:** Active Directory (member/memberOf schema) (dropdown menu)
- Проверка подлинности:** Анонимный доступ (dropdown menu)
- Buttons: [Добавить сервер](#) and [Удалить домен](#)

Шаг 3. Подтвердить удаление домена нажатием [OK](#) в диалоговом окне

The screenshot shows a confirmation dialog box with the text: "Вы уверены, что хотите удалить этот домен из списка?". At the bottom, there are two buttons: [OK](#) and [Отмена](#).

Шаг 4. Сохранить настройки [Сохранить](#).

При успешном сохранении настроек появится оповещение

Конфигурация успешно обновлена

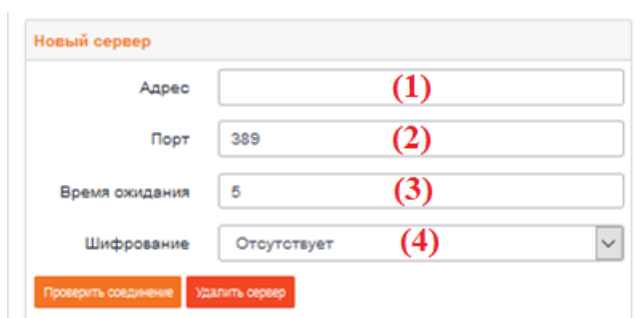
7.4.2 Сервер LDAP

7.4.2.1 Добавление сервера LDAP

Для добавления нового сервера LDAP необходимо:

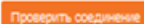
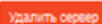
Шаг 1. В разделе **Настройки**>**Настройки LDAP** нажать  .

Шаг 2. В появившейся форме выбрать **домен LDAP**, куда необходимо добавить сервер, и нажать  .



Новый сервер

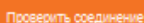
Адрес	<input type="text"/>	(1)
Порт	<input type="text" value="389"/>	(2)
Время ожидания	<input type="text" value="5"/>	(3)
Шифрование	<input type="text" value="Отсутствует"/>	(4)

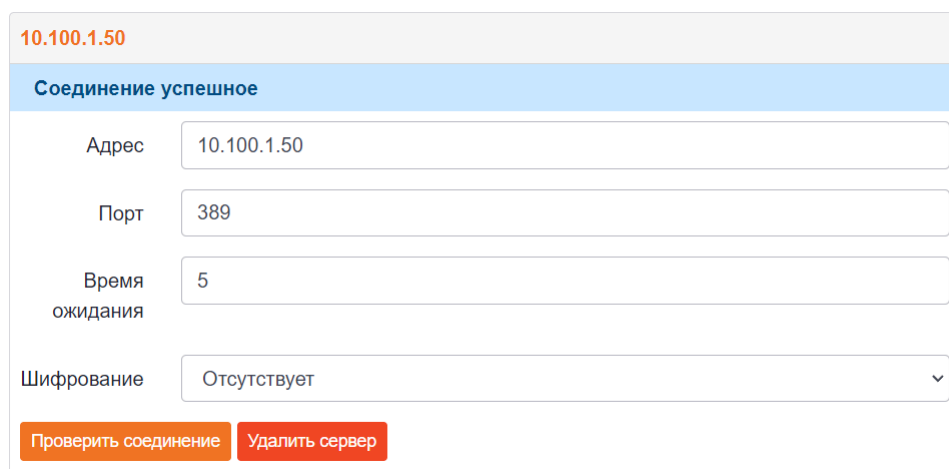
 

Шаг 3. Заполнить необходимые поля:

- (1) – IP-адрес сервера LDAP;
- (2) – порт;
- (3) – время ожидания;
- (4) – шифрование.





Соединение с сервером можно проверить в любое время нажатием на кнопку в соответствующем разворачивающемся блоке  .




10.100.1.50

Соединение успешное

Адрес	<input type="text" value="10.100.1.50"/>
Порт	<input type="text" value="389"/>
Время ожидания	<input type="text" value="5"/>
Шифрование	<input type="text" value="Отсутствует"/>

Шаг 4. Сохранить настройки  .


При успешном сохранении настроек появится оповещение

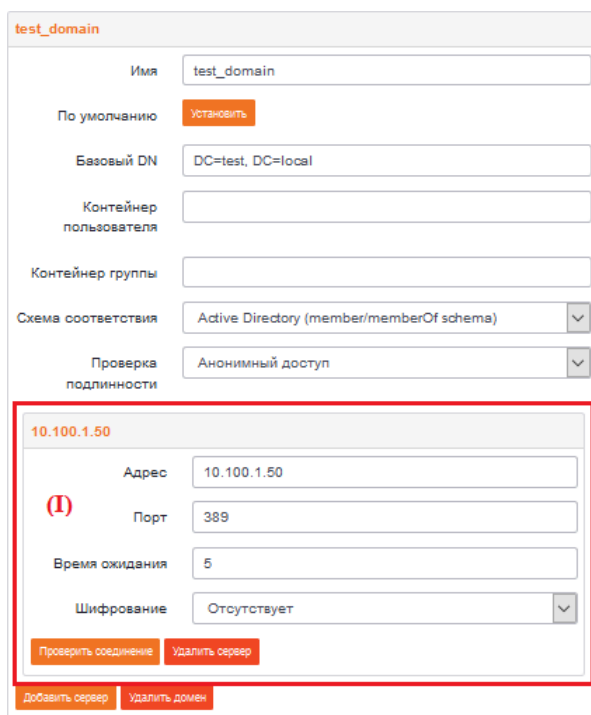
Конфигурация успешно обновлена

7.4.2.2 Удаление сервера LDAP

Для удаления сервера LDAP необходимо:


Шаг 1. В разделе **Настройки>Настройки LDAP** нажать  .

Шаг 2. В появившейся форме выбрать соответствующий домен LDAP и нажать  в области соответствующего сервера (I)



test_domain

Имя test_domain

По умолчанию 

Базовый DN DC=test, DC=local

Контейнер пользователя

Контейнер группы

Схема соответствия Active Directory (member/memberOf schema)

Проверка подлинности Анонимный доступ

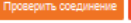

10.100.1.50



Адрес 10.100.1.50

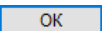
(I) Порт 389

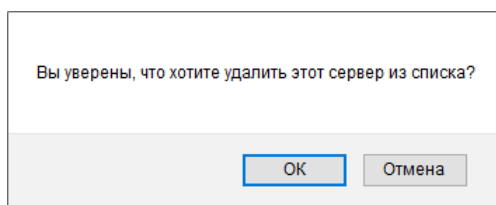
Время ожидания 5

Шифрование Отсутствует

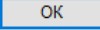

 

Шаг 3. Подтвердить удаление домена нажатием  в диалоговом окне

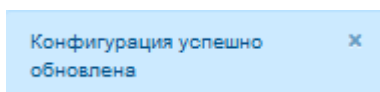


Вы уверены, что хотите удалить этот сервер из списка?

Шаг 4. Сохранить настройки  .

При успешном сохранении настроек появится оповещение



7.4.3 Группы LDAP

7.4.3.1 Привязка группы LDAP к роли

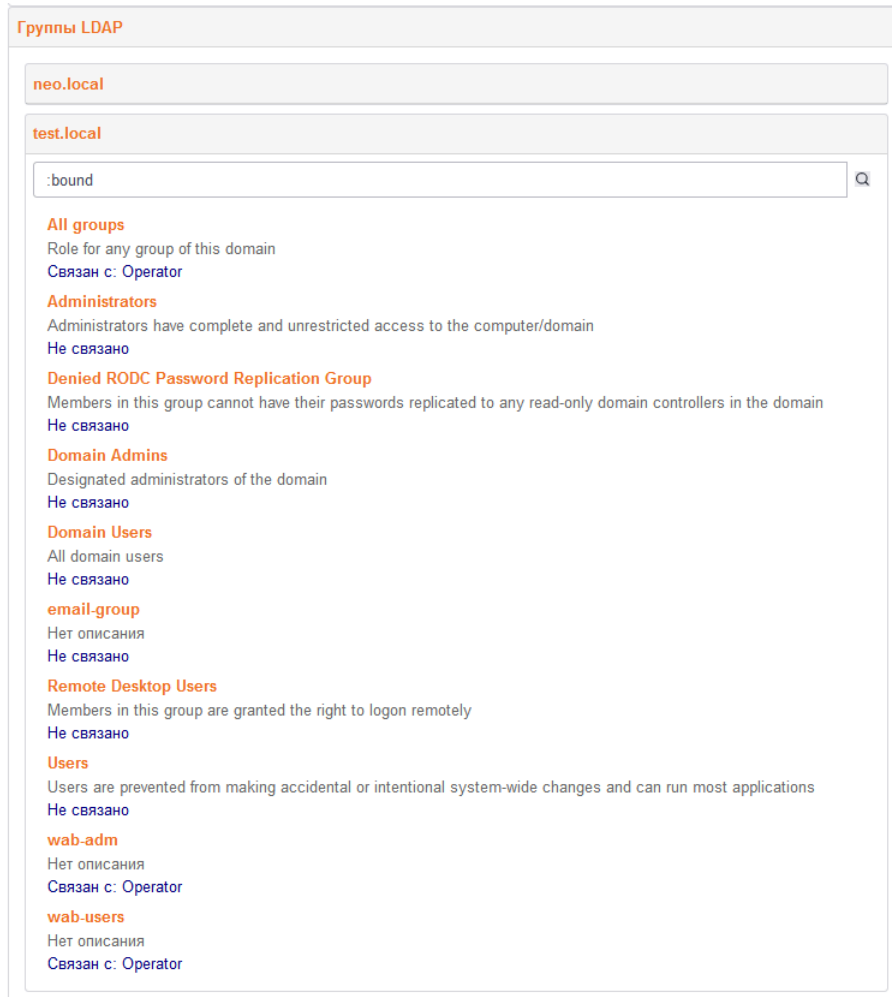
СКДПУ НТ позволяет ассоциировать группы LDAP с ролями, определенными в СКДПУ НТ. Для этого следует выполнить следующие шаги:

Шаг 1. В разделе **Настройки>Настройки LDAP** нажать  .

Шаг 2. Раскрыть список групп LDAP и выбрать требуемый домен



Шаг 3. Раскрыть домен нажатием на нем левой кнопки мыши



Шаг 4. Для группы выбрать требуемую роль из выпадающего списка и привязать нажатием

Шаг 5. Сохранить настройки **Сохранить** .

В результате у выбранной группы LDAP появится привязка к роли СКДПУ НТ.



Соединение с сервером можно проверить в любое время нажатием в соответствующем выпадающем элементе **Проверить соединение** .

При успешном сохранении настроек появится оповещение

Конфигурация успешно обновлена

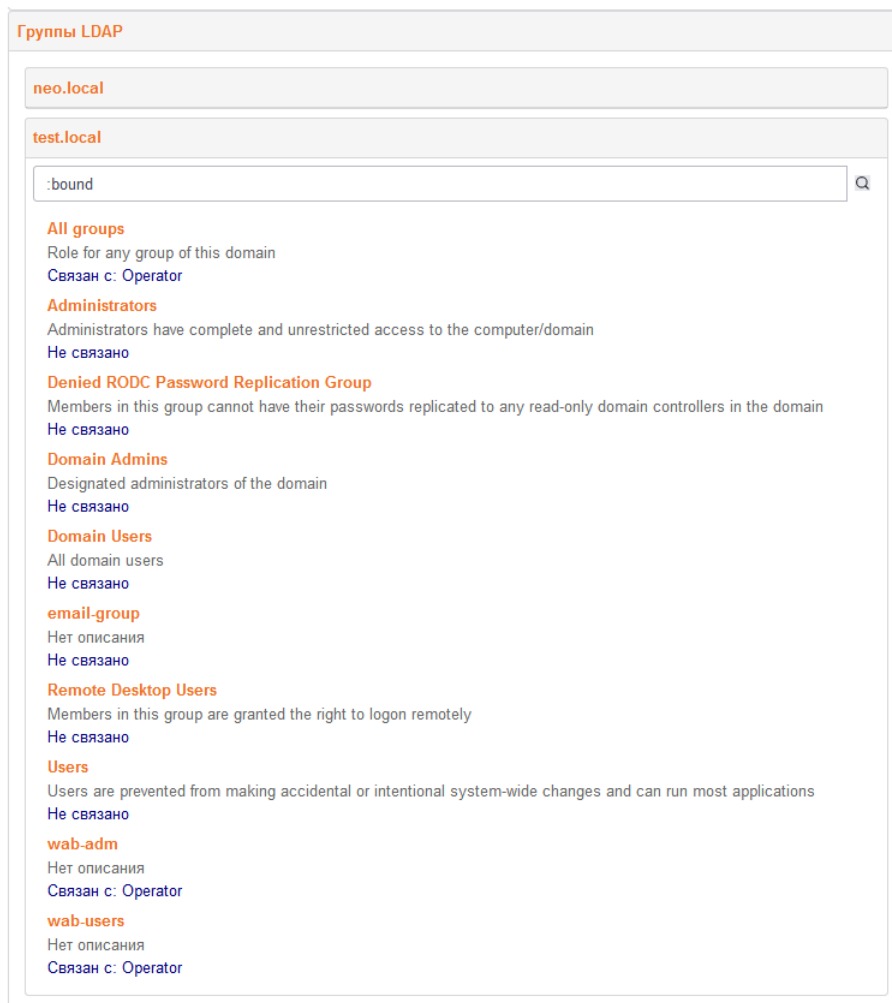
7.4.3.2 Удаление привязки группы LDAP к роли

Для того, чтобы отвязать выбранную группу LDAP от роли СКДПУ НТ необходимо выполнить следующие шаги:

Шаг 1. В разделе **Настройки > Настройки LDAP** нажать **Редактировать** .

Шаг 2. Раскрыть список групп LDAP и выбрать требуемый домен

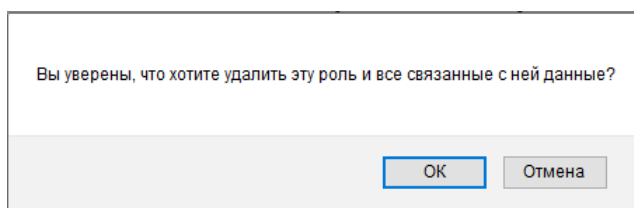
Шаг 3. Раскрыть домен нажатием на нем левой кнопки мыши



Шаг 4. Для группы выбрать требуемую роль из выпадающего списка и привязать нажатием

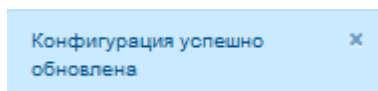
Отвязать роль

Шаг 5. Подтвердить удаление привязки



Шаг 6. Сохранить настройки **Сохранить**.

При успешном сохранении настроек появится оповещение



7.5 Конфигурация журналирования

В рассматриваемом разделе администратор СКДПУ НТ имеет возможность настроить передачу различных типов записей журнала СКДПУ НТ на удаленные серверы. Администратор

должен указать IP-адрес сервера (1), порт, по которому будет происходить передача (2), и протокол (3), а также выбрать формат записи журнала (4) и тип записей журнала (5) (см. [рисунок 12](#)).



По умолчанию все данные аудита безопасности будут храниться на сервере, где установлен СКДПУ НТ.

Рисунок 12 – Раздел Настройки > Конфигурация журналирования

В СКДПУ НТ генерируются следующие записи журналов:

- данные об авторизации пользователей СКДПУ НТ (authorization);
- данные аудита безопасности СКДПУ НТ (audit);
- данные пользовательских сессий СКДПУ НТ (session);
- данные об обнаруженных инцидентах (incidents).

7.5.1 Добавить подключение к удаленному серверу

Для добавления подключения к удаленному серверу необходимо:

Шаг 1. В разделе **Настройки > Конфигурация журналирования** в соответствующие поля внести данные о параметрах настройки сервера, а также данные о формате записей и типе журнала

- (1) – отметка об активности подключения к удаленному серверу;
- (2) – адрес удаленного сервера;
- (3) – порт подключения к удаленному серверу;
- (4) – протокол передачи данных на удаленный сервер (UDP, TCP, TLS);
- (5) – формат передачи данных (RFC, ISO);
- (6) – выбор типа передаваемых данных (authorization, audit, session).

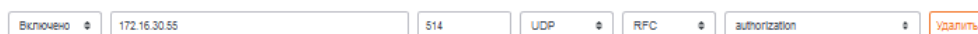
Шаг 2. Нажать .

Шаг 3. Для сохранения внесенных изменений нажать .

7.5.2 Удалить подключение к удаленному серверу

Для удаления подключения к удаленному серверу необходимо:

Шаг 1. В разделе **Настройки>Конфигурация журналирования** в строке выбранного подключения нажать **Удалить**.

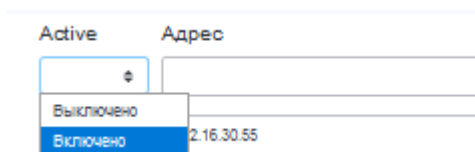


Шаг 2. Для сохранения внесенных изменений нажать **Применить настройки**.

7.5.3 Активировать/деактивировать подключение к удаленному серверу

Для изменения статуса подключения к удаленному серверу необходимо:

Шаг 1. В разделе **Настройки>Конфигурация журналирования** в выпадающем списке выбрать необходимый статус подключения



Шаг 2. Для сохранения внесенных изменений нажать **Применить настройки**.

7.6 Информация о лицензии

В данном разделе администратор СКДПУ НТ имеет возможность добавить файл лицензии **Добавить лицензию**, чтобы получить доступ к той части функционала СКДПУ НТ, которая будет доступна в соответствии с выданной лицензией (см. [раздел 11.5](#)).

Также предоставляется возможность скачать используемую в СКДПУ НТ лицензию нажатием на **Скачать лицензию**.




При отсутствии лицензии доступ к СКДПУ НТ будет разрешен, но в веб-интерфейсе появится соответствующее сообщение.

LICENSE ISSUE

8 ЦЕЛЕВЫЕ СИСТЕМЫ

8.1 Общие сведения

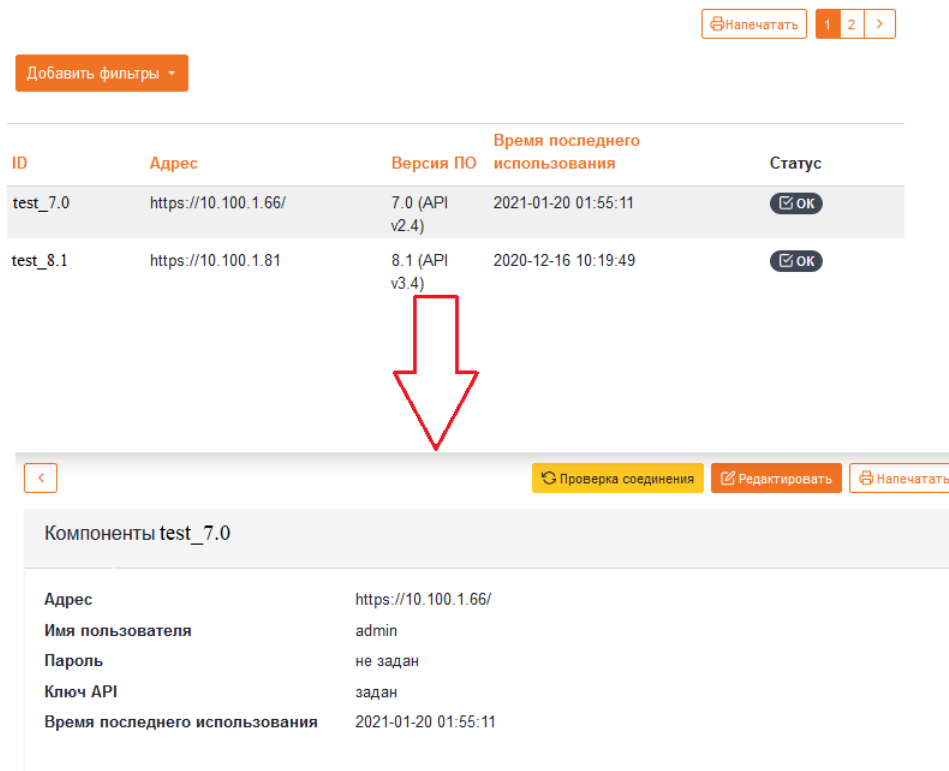
СКДПУ НТ предоставляет возможность администратору настраивать аутентификацию шлюзов для подключения к целевым системам в целях получения данных пользовательских сессий целевых систем.

 Действия по организации подключения целевых систем к СКДПУ НТ приведены в разделе 6.1

8.2 Настройка аутентификации шлюзов

Для настройки аутентификации шлюзов необходимо:



Шаг 1. В разделе веб-интерфейса **Компоненты**>**Шлюзы** выбрать шлюз из списка нажатием левой кнопки мыши



ID	Адрес	Версия ПО	Время последнего использования	Статус
test_7.0	https://10.100.1.66/	7.0 (API v2.4)	2021-01-20 01:55:11	
test_8.1	https://10.100.1.81	8.1 (API v3.4)	2020-12-16 10:19:49	

Компоненты test_7.0

Адрес	https://10.100.1.66/
Имя пользователя	admin
Пароль	не задан
Ключ API	задан
Время последнего использования	2021-01-20 01:55:11

 Имеется возможность проверить соединение со шлюзом, нажав на 

Шаг 2. Нажать 

Шаг 3. В появившейся форме изменить параметры аутентификации шлюза




Имеется возможность указать способ аутентификации по паролю и по ключу API.

The screenshot shows a configuration form for a gateway named 'test_7.0'. The form is divided into several sections:

- Адрес:** A text input field containing 'https://10.100.1.66/' with a red circled '1' next to it.
- Имя пользователя:** A text input field containing 'admin' with a red circled '2' next to it.
- Пароль:** A text input field containing 'Пароль не установлен' with a red circled '3' next to it.
- Подтверждение пароля:** An empty text input field.
- Ключ API:** A text input field containing 'Токен API установлен' with a red circled '4' next to it.
- Подтверждение токена:** An empty text input field.
- Сбросить:** A checkbox labeled 'Сбросить' is present below both the password and API key sections.
- Сохранить:** An orange button labeled 'Сохранить' is located at the bottom left of the form.

В рассматриваемой форме ввести необходимую информацию :

- (1) – URL шлюза;
- (2) – имя пользователя, под которым осуществляется вход на шлюз;
- (3) – аутентификация по паролю (необходима для доступа к записям пользовательских сессий на целевых системах);
- (4) – аутентификация по ключу API (необходима для просмотра видео записей пользовательских сессий на целевых системах).

Шаг 4. Для сохранения внесенных изменений необходимо нажать  .

При успешном изменении параметров шлюза появится оповещение

Данные шлюза обновлены x

9 АУДИТ БЕЗОПАСНОСТИ

9.1 Общие сведения

В СКДПУ НТ осуществляется аудит следующих событий безопасности:

- начало и завершение сессий пользователей СКДПУ НТ;
- любые попытки идентификации и аутентификации (успешные и неуспешные) пользователей СКДПУ НТ;
- создание, изменение и удаление учетных записей пользователей СКДПУ НТ;
- создание, изменение и удаление ролей пользователей СКДПУ НТ;
- блокирование и разблокирование пользователей СКДПУ НТ;
- изменение пароля пользователя СКДПУ НТ;
- изменение настроек детекторов аномального поведения пользователей на целевых системах (детекторов аномалий);
- изменение данных инцидента, инициированного по результатам анализа данных пользовательской сессии на целевых системах;
- просмотр данных пользовательской сессии на целевых системах в СКДПУ НТ;
- создание, изменение и отправка отчетов средствами СКДПУ НТ;
- изменение настроек СКДПУ НТ;
- перезапуск сервисов СКДПУ НТ.

Записи событий имеют формат SEF и содержат следующую информацию:

- тип события;
- дата и время события;
- IP-адрес сервера СКДПУ НТ;
- идентификатор пользователя СКДПУ НТ;
- категория события;
- критичность события.

Записи событий безопасности, в зависимости от регистрируемого события, должны содержать следующую дополнительную информацию:

Событие	Дополнительная информация
Начало сессии пользователя СКДПУ НТ	Время открытия сессии, IP-адрес источника (пользователя СКДПУ НТ) события
Неудачная авторизация пользователя СКДПУ НТ	IP-адрес источника (пользователя СКДПУ НТ) события
Завершение сессии пользователя СКДПУ НТ	Время закрытия сессии; IP-адрес источника (пользователя СКДПУ НТ) события
Управление учетными записями пользователей СКДПУ НТ	Идентификатор пользователя СКДПУ НТ, ассоциированного с учетной записью

Событие	Дополнительная информация
Управление ролями СКДПУ НТ	Идентификатор роли СКДПУ НТ
Управление блокированием пользователей СКДПУ НТ	Идентификатор заблокированного или разблокированного пользователя СКДПУ НТ
Изменение пароля пользователя СКДПУ НТ	Идентификатор пользователя СКДПУ НТ, с которым ассоциируется пароль
Изменение настроек детекторов аномалий	Состав изменений в формате списка «ключ-значение»; IP-адрес источника (пользователя СКДПУ НТ) события
Изменение данных инцидента	Состав изменений в формате списка «ключ-значение»; IP-адрес источника (пользователя СКДПУ НТ) события
Просмотр данных пользовательских сессий целевых систем	Идентификатор просматриваемого пользователя целевой системы
Создание, изменение и отправка отчетов средствами СКДПУ НТ	Наименование отчета
Изменение настроек СКДПУ НТ	Состав изменений в формате списка «ключ-значение»
Перезапуск сервисов СКДПУ НТ	Наименование сервиса

Записи регистрируемых событий фиксируются в соответствующих журналах, расположенных в директории `/opt/skdpu-nt-data/log`.



В веб-интерфейсе СКДПУ НТ имеется возможность просмотра только записей журнала авторизаций (см. [раздел 9.2](#)).

9.2 Журнал авторизаций

Администратор может ознакомиться со статистикой успешных и неуспешных попыток идентификации и аутентификации пользователей СКДПУ НТ, перейдя в раздел **Отчеты>Журнал авторизаций**, см. [рисунок 13](#).

Отчёты Библиотека отчётов История выполнения Профили выполнения **Журнал авторизаций**

1 2 3 4 5 ... 61 62 >

Добавить фильтры ▾

Зарегистрирован	Пользователь/логин	Действие	Данные
2021-02-17 12:27:51	admin	login	client: 192.168.20.93
2021-02-17 12:09:16	admin	login	client: 192.168.20.93
2021-02-17 12:09:11	admin	login failed	client: 192.168.20.93
2021-02-17 11:38:34	test_user	login	client: 192.168.20.93
2021-02-17 11:38:27	admin	logout	client: 192.168.20.93
2021-02-17 11:38:03	admin	login	client: 192.168.20.93
2021-02-17 11:37:58	test_user	logout	client: 192.168.20.93
2021-02-17 11:37:07	test_user	login	client: 192.168.20.93
2021-02-17 11:37:02	admin	logout	client: 192.168.20.93
2021-02-17 11:36:00	admin	login	client: 192.168.20.93
2021-02-17 03:44:58	star	login	client: 172.16.30.63
2021-02-17 03:44:45	admin	login failed	client: 172.16.30.63
2021-02-16 19:24:43	admin	login	client: 172.16.30.63
2021-02-16 18:39:29	admin	login	client: 172.16.30.63
2021-02-16 18:37:06	admin	login	client: 172.16.30.63
2021-02-16 18:15:15	admin	login	client: 172.16.30.63
2021-02-16 18:09:32	admin	login	client: 172.16.30.63
2021-02-16 17:51:55	admin	login	client: 172.16.30.63
2021-02-16 17:46:11	admin	login	client: 172.16.30.63
2021-02-16 17:36:51	admin	login	client: 172.16.30.63
2021-02-16 17:36:29	admin	login	client: 172.16.30.63
2021-02-16 17:29:05	admin	login	client: 172.16.30.63
2021-02-16 17:23:43	admin	login	client: 192.168.20.93
2021-02-16 17:20:34	admin	login	client: 172.16.30.63
2021-02-16 17:03:20	admin	login	client: 172.16.30.63

1 2 3 4 5 ... 61 62 >

Рисунок 13 – Раздел Отчеты > Журнал авторизаций

10 СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

10.1 Добавление LDAP-домена

Описание сценария

Добавление нового LDAP-домена.

Условия для успешного выполнения

- Успешное добавление возможно только при правильном указании настроек.

Сценарий

Шаг 1. Авторизоваться в веб-интерфейсе СКДПУ НТ.

Шаг 2. Перейти в раздел интерфейса **Настройки > Настройки LDAP** и открыть раздел на редактирование, нажав на кнопку **Редактировать**.

Шаг 3. Нажать на кнопку **Добавить новый домен** и в открывшейся форме заполнить поля данными домена.

Шаг 4. Нажать на кнопку **Сохранить**.



В списке доменов LDAP появится новая запись.

10.2 Добавление LDAP-сервера

Описание сценария

Добавление нового LDAP-сервера.

Условия для успешного выполнения

- Успешное добавление возможно только при правильном указании настроек.

Сценарий

Шаг 1. Авторизоваться в веб-интерфейсе СКДПУ НТ.

Шаг 2. Перейти в раздел интерфейса **Настройки > Настройки LDAP** и открыть раздел на редактирование, нажав на кнопку **Редактировать**.

Шаг 3. Нажать на кнопку **Добавить сервер** в группе элементов интерфейса добавляемого или существующего LDAP-домена.

Шаг 4. В открывшейся форме заполнить поля данными сервера.

Шаг 5. Для проверки соединения с LDAP-сервером нажать на кнопку **Проверить соединение**. Проверка соединения занимает некоторое время. Результат проверки отображается в заголовке блока.



LDAP-сервер добавлен к домену.

10.3 Добавления роли

Описание сценария

Создание и настройка роли, которая должны быть у пользователей доменных групп.

Условия для успешного выполнения

- При добавлении роли необходимо выбрать хотя бы одно разрешение.

Сценарий

Шаг 1. Авторизоваться в веб-интерфейсе СКДПУ НТ.

Шаг 2. Перейти в раздел интерфейса **Права доступа** > **Роли** и открыть раздел на добавление, нажав на кнопку **Добавить роль**.

Шаг 3. В поле **Роль** ввести название роли, ниже отметить функционал и разделы интерфейса доступные данной роли.

Шаг 4. Сохранить созданную роль нажатием на кнопку **Сохранить**.



В списке ролей появится новая запись.

10.4 Связывание роли и доменной группы

Описание сценария

Создание связи между ролью и доменной группой пользователей.

Условия для успешного выполнения

- Роль и доменная группа должны быть созданы заранее.

Сценарий

Шаг 1. Авторизоваться в веб-интерфейсе СКДПУ НТ.

Шаг 2. Перейти в раздел интерфейса **Права доступа** > **Группы LDAP** и открыть раздел на редактирование, нажав на кнопку **Редактировать**.

Шаг 3. Нажать на название домена, группу которого необходимо связать с ролью, при этом открывается окно поиска группы и список уже связанных групп, если такие есть.

Шаг 4. В поле с отметкой **:bound** ввести целиком или частично **название доменной группы** и нажать на кнопку **Поиск** справа от поля.

Шаг 5. Нажать на искомую группу в перечне результатов поиска, после этого откроется выпадающий список с перечнем ролей, доступных для связывания.

Шаг 6. Выбрать созданную ранее роль и подтвердить связывание нажатием на кнопку **Привязать роль**.

Шаг 7. Сохранить произведенные настройки нажатием на кнопку **Сохранить**.



Создана связь роли и доменной группы.

11 ОБСЛУЖИВАНИЕ СКДПУ НТ

В рассматриваемом разделе приводится описание процедур по обслуживанию СКДПУ НТ и устранению часто возникающих проблем.

11.1 Диагностика СКДПУ НТ и его сервисов

СКДПУ НТ с помощью веб-интерфейса в разделе **Диагностика** предоставляет возможность администратору СКДПУ НТ осуществлять мониторинг и диагностику состояния сервера СКДПУ НТ и его системных процессов (сервисов) (см. [рисунок 14](#)).

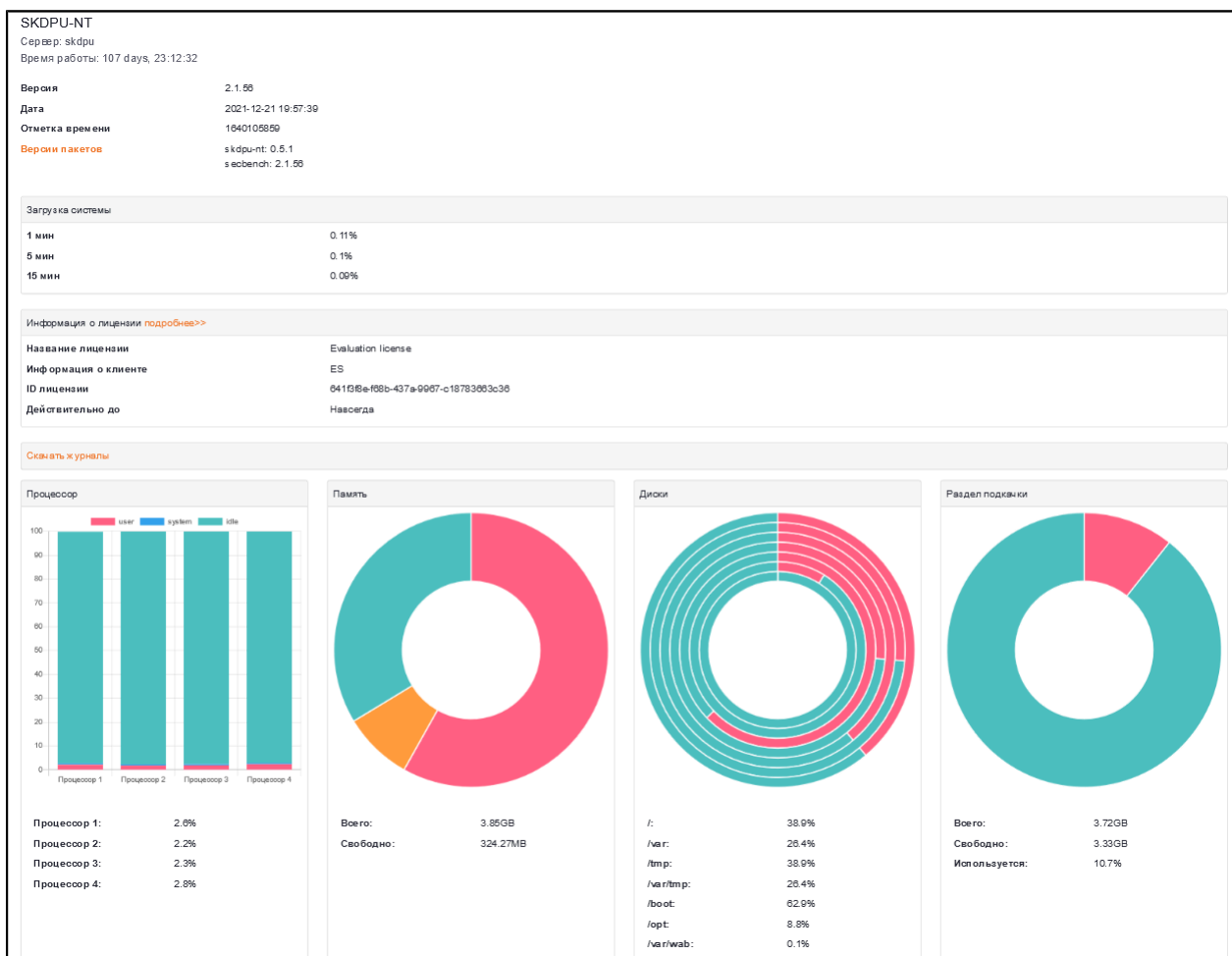


Рисунок 14 – Раздел Диагностика

В [таблице 4](#) представлен перечень сервисов, доступных для управления из веб-интерфейса СКДПУ НТ.

Таблица 4 – Доступные для управления сервисы

Наименование сервиса	Описание
analysed	Оповещение о поступлении на обработку новых данных пользовательских сессий и проведение анализа на предмет наличия признаков аномального поведения пользователей шлюзов доступа. Регистрация обнаруженных инцидентов

Наименование сервиса	Описание
collectd	Обработка полученных данных пользовательских сессий целевых систем от доступных шлюзов доступа, регистрация обнаруженных событий
indexd	Индексирование данных пользовательских сессий целевых систем, поступающих от шлюзов доступа, и их размещение в среде функционирования в виде текстовых файлов
enrichd	Регистрация событий безопасности, получаемых от систем сторонних производителей
jobrunnerd	Генерирование отчетов, структура которых соответствует предварительно выбранным шаблонам, и их отправка по электронной почте в соответствии с выбранными профилями выполнения

Для каждого сервиса отображается информация о его текущем статусе (**Статус**), идентификаторе (**PID**), потребляемых ресурсах центрального процессора (**Процессор**), а также о потребляемом объеме физической RAM (**rss**) и виртуальной (**vms**) памяти. При необходимости администратор СКДПУ НТ имеет возможность осуществить перезапуск компонентов СКДПУ НТ. Пример одного из сервисов СКДПУ НТ (см. [рисунок 15](#)).

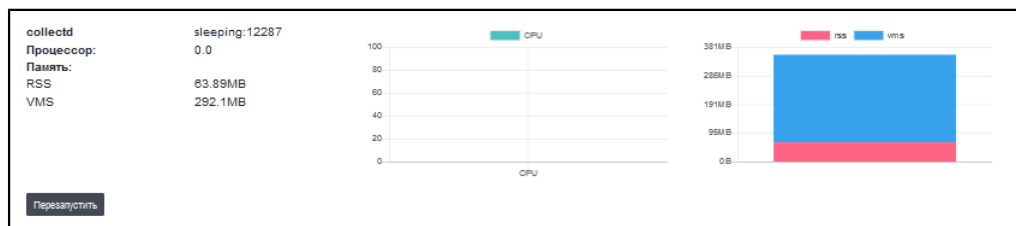


Рисунок 15 – Статистика компонента collectd

11.2 Диагностика СКДПУ НТ через консоль ОС

Диагностику СКДПУ НТ можно осуществить через консоль ОС посредством утилиты `/opt/skdpu-nt/bin/nt-status`

```
root@skdpunt-test1:/var/log# /opt/skdpu-nt/bin/nt-status
Server: skdpunt-test1
Uptime: 1 day, 5:05:09.504636
Load averages: 0.08 0.02 0.01
CPU: 2 cores detected
      0      65.0     14.0
      1      0.0      0.0
Total memory: 1.95GB
Available: 1.41GB
Used: 546.11MB 27.4%
Swap: 2.0GB
Free: 2.0GB 0.1%
Filesystem: /
Total: 76.27GB
Used: 2.15GB 3.0%
Process: collectd is running (8317)
CPU usage: 0.0%
Memory usage: 284.07MB
Process: analysed is running (8285)
CPU usage: 0.0%
Memory usage: 285.68MB
root@skdpunt-test1:/var/log#
```



Для доступа к консоли ОС администратору СКДПУ НТ необходимо обладать правами администратора ОС.

11.3 Сброс пароля администратора веб-интерфейса СКДПУ НТ

При возникновении нештатной ситуации, когда невозможно получить доступ к функциональным возможностям через веб-интерфейс СКДПУ НТ с помощью встроенной учетной записи `admin`, необходимо сбросить пароль для возобновления доступа. Для этого необходимо:

- Шаг 1. В консоли ОС сервера, где установлен СКДПУ НТ, войдите в режим суперпользователя.
- Шаг 2. Запустите утилиту для сброса пароля администратора до значения по умолчанию (пароль: `admin`)

```
/opt/skdpu-nt/bin/nt-restore-default-admin -f
```

11.4 Смена паролей учетных записей консоли администрирования

Для смены паролей учетных записей `ntadmin` и `ntsuper` используют штатную команду `passwd` в консоли ОС.

11.5 Добавление файла лицензии

Чтобы загрузить переданный файл лицензии необходимо:

- Шаг 1. Войти в консоль администрирования под учетной записью `ntadmin`.
- Шаг 2. Получить права суперпользователя.
- Шаг 3. Скопировать предоставленный файл лицензии `<file.key>` на сервер СКДПУ НТ в директорию `/home/ntadmin/`, используя клиент SCP или SFTP.

Шаг 4. Перенести файл лицензии командой

```
mv /home/ntadmin/<file.key> /opt/skdpu-nt/etc/license.key
```

Шаг 5. Перезапустить сервисы apache2 и gunicorn

```
systemctl restart apache2  
systemctl restart gunicorn
```

Шаг 6. Авторизоваться в веб-интерфейсе СКДПУ НТ.

Шаг 7. Перейти в раздел **Настройки > Информация о лицензии**, где должны появиться сведения об установленной лицензии.

11.6 Резервное копирование и восстановление параметров

11.6.1 Создание резервных копий

Для создания резервных копий администратору СКДПУ НТ необходимо:

Шаг 1. В консоли ОС сервера, где установлен СКДПУ НТ, войти в режим суперпользователя.

Шаг 2. Для создания резервной копии настроек СКДПУ НТ необходимо запустить утилиту:

```
/opt/skdpu-nt/bin/nt-backup-settings archive_name
```

archive_name

путь к архиву

Резервные копии файлов с настройками будут размещены в `archive_name`.

Шаг 3. Для создания резервной копии данных инцидентов и сессий, хранящихся в СКДПУ НТ, необходимо запустить утилиту:

```
/opt/skdpu-nt/bin/nt-data-backup -r
```

Резервные копии данных сессий и инцидентов будут размещены в `/opt/skdpu-nt-data/backup/backup-host_name-YYYYMMddhhmmss/`, где

host_name

имя сервера СКДПУ НТ

YYYYMMdd

дата формирования резервной копии

hhmmss

время формирования резервной копии



Процедуру резервного копирования рекомендуется проводить, как минимум, один раз в месяц.

11.6.2 Восстановление из резервных копий

Для восстановления данных администратору СКДПУ НТ необходимо:

Шаг 1. В консоли ОС сервера, где установлен СКДПУ НТ, войти в режим суперпользователя.

Шаг 2. Выполнить утилиту

```
/opt/skdpu-nt/bin/nt-data-restore -a ARCHIVE
```

В результате данные будут восстановлены и помещены в соответствующие директории. Если данных много, системе потребуется время, чтобы по ним был построен поисковый индекс.



Архивы могут содержать чувствительную информацию, такую как пароли. СКДПУ НТ не производит шифрования или другого кодирования архивов резервных копий, поэтому следует надежно хранить резервные копии и не предоставлять бесконтрольно к ним доступ

11.7 Удаление устаревших данных пользовательских сессий целевых систем

Администратор СКДПУ НТ имеет возможность задать период удаления устаревших данных пользовательских сессий (какие данные считать устаревшими определяет администратором).

Для удаления данных необходимо:

Шаг 1. В консоли ОС сервера, где установлен СКДПУ НТ, войти в режим суперпользователя.

Шаг 2. Выполнить утилиту

```
/opt/skdpu-nt/bin/nt-data-rotate -d DATE
```



Рекомендуется перед выполнением ротации выполнять резервное копирование данных (см. [раздел 11.6.1](#)).

11.8 Обновление СКДПУ НТ

Стандартный режим обновления представляет собой установку новых версий пакетов из предоставляемого дистрибутива. Необходимо выполнить следующие шаги:

Шаг 1. В консоли ОС сервера, где установлен СКДПУ НТ, войти в режим суперпользователя.

Шаг 2. Скопировать пакеты из предоставленного дистрибутива на сервер СКДПУ НТ.

Шаг 3. Настроить новый источник пакетов дистрибутива в файле `/etc/apt/sources.list`.

Шаг 4. Обновить СКДПУ НТ посредством выполнения команды

```
apt-get install skdpu-nt
```

Шаг 5. Запустить утилиту

```
/opt/skdpu-nt/bin/nt-data-rotate -d DATE
```



Компоненты СКДПУ НТ с большой вероятностью будут приостановлены на время процедуры обновления, вследствие чего процедура анализа инцидентов также будет приостановлена. Полученные во время процедуры обновления данные пользовательских сессий целевых систем будут сохранены и обработаны впоследствии.

11.9 Обращение в службу поддержки

Для формирования необходимого набора информации в целях передачи в службу технической поддержки администратор СКДПУ НТ должен выполнить следующие шаги:

Шаг 1. В консоли ОС сервера, где установлен СКДПУ НТ, войти в режим суперпользователя.

Шаг 2. Выполнить утилиту

```
/opt/skdpu-nt/bin/nt-support-bundle target
```

В результате будет создан архив, состоящий из текстовых файлов, которые можно будет передать в службу технической поддержки производителя, при необходимости проконтролировав содержимое визуально.

Также администратор СКДПУ НТ собирает необходимую информацию с использованием веб-интерфейса:

Шаг 1. В разделе **Диагностика** раскрыть выпадающий элемент **Создать журналы**

Дата создания	Размер	
20.01.2020, 10:59:43	1MB	Скачивание
20.01.2020, 10:59:53	1MB	Скачивание
23.01.2020, 15:56:15	2MB	Скачивание
28.01.2020, 01:18:06	555KB	Скачивание
06.02.2020, 21:43:39	5MB	Скачивание
26.03.2020, 20:52:14	6MB	Скачивание
13.05.2020, 17:26:33	141MB	Скачивание

Создать новый архив

Шаг 2. Нажать **Создать новый архив**.

Шаг 3. Выбрать расположение для его сохранения в системе.



Для скачивания ранее созданных архивов журналов необходимо напротив выбранного архива нажать **Скачивание** с последующим указанием расположения для сохранения в системе.

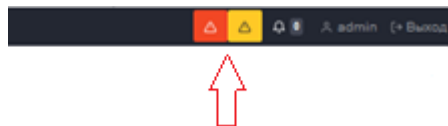
Созданные архивы включает в себя следующие файлы:

-
- системные журналы ОС;
 - журналы СКДПУ НТ;
 - основные параметры состояния ОС (имя хоста, адрес и другие настройки сети, дату и время, загрузку CPU и RAM, свободное место для хранения в рамках ОС), ключевые параметры работоспособности СКДПУ НТ, например информацию о наличии необходимых сервисов, срез показателей производительности и информацию о наличии критических ошибок от средств внутреннего мониторинга системы на момент подготовки архива.

12 ВОЗМОЖНЫЕ ВОПРОСЫ

В данном разделе рассмотрены вопросы, которые могут произойти в процессе эксплуатации СКДПУ НТ.

При возникновении нештатных ситуаций в процессе функционирования СКДПУ НТ происходит сигнализация в веб-интерфейсе СКДПУ НТ посредством отображения соответствующих иконок на панели, расположенной в верхней части веб-интерфейса:



i Сведения об вопросах, возникающих в процессе функционирования СКДПУ НТ, заносятся в соответствующий журнал `/opt/skdpu-nt/var/log/errors`.



12.1 Нарушение целостности компонентов СКДПУ НТ

СКДПУ НТ посредством сигнализирования в веб-интерфейсе СКДПУ НТ. При нажатии на иконку происходит переход в раздел веб-интерфейса СКДПУ НТ **Диагностика**, где можно ознакомиться с подробной информацией об ошибке

```
Integrity violations
Checksum mismatch for /opt/skdpu-nt/lib/python3.5/site-packages/gui/templates/incidents/show.html: stored =
60c8c29340a0d2921ba07ebf0bf52ec4ed2ce400, calculated = 9baca26f3f88158451f8e11b0ceab14195743f90
```

12.2 Недостаток свободного места в хранилище

При возникновении дефицита свободного места на сервере СКДПУ НТ для хранения журналов и данных пользовательских сессий целевых систем происходит сигнализирование в веб-интерфейсе посредством отображения следующих иконок:

-  отображается при уменьшении количества свободного места ниже 20% от общего объема хранилища;
-  отображается при уменьшении количества свободного места ниже 10% от общего объема хранилища.

i При заполнении хранилища более, чем на 95% от общего объема, прием записей журналов и данных пользовательских сессий целевых систем прекращается.

При нажатии на иконки происходит переход в раздел веб-интерфейса СКДПУ НТ **Диагностика**.

```
Integrity violations
Checksum mismatch for /opt/skdpu-nt/lib/python3.5/site-packages/gui/templates/incidents/show.html: stored =
60c8c29340a0d2921ba07ebf0bf52ec4ed2ce400, calculated = 9baca26f3f88158451f8e11b0ceab14195743f90
```

Для освобождения хранилища необходимо удалить устаревшие данные (см. [раздел 11.7](#)), а затем запустить прием данных пользовательских сессий целевых систем в разделе **Диагностика** (см. [рисунок 16](#))

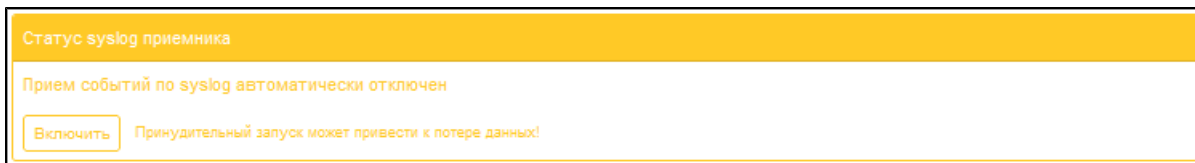


Рисунок 16 – Статус приемника

12.3 Отсутствие файла лицензии

После установки может быть ситуация, когда не был загружен файл лицензии в СКДПУ НТ, при этом кнопка [↓ Скачать лицензию](#) активна.

Попытка скачать файл лицензии выведет сообщение об ошибке.

В этом случае необходимо незамедлительно связаться со службой технической поддержки для устранения проблемы.

Приложение

А

ПЕРЕЧЕНЬ УТИЛИТ КОНСОЛИ АДМИНИСТРИРОВАНИЯ СКДПУ NT

Описание встроенных утилит СКДПУ NT и их параметров

nt-backup-settings

Создание архива с настройками СКДПУ NT

```
nt-backup-settings [-h] [-v] [-a ADD_FILE] [-o OWNERSHIP] archive_name
```

-h

вывод справки

-v

вывод на консоль логов в процессе выполнения утилиты

-a ADD_FILE

флаг добавления файла *ADD_FILE* в архив настроек (можно указать несколько файлов)

-o OWNERSHIP

флаг прав *OWNERSHIP* на файл архива

archive_name

имя архива

nt-check-expiration

Контроль окончания срока действия паролей и учетных записей пользователей СКДПУ NT

```
nt-check-expiration [-h] [-c CONFIG] [-v] -r
```

-h

вывод справки

-v

вывод на консоль логов в процессе выполнения утилиты

-c CONFIG

выбор конфигурационного файла *CONFIG*

-r

без указания этого параметра действия выполняться не будут

nt-check-storage

Контроль объема свободной памяти локального хранилища данных

```
nt-check-storage
```

nt-config-tool

Утилита для обновления файлов конфигурации. Вызывается при установке новых версий программного обеспечения

```
nt-config-tool [-h] [-v] {merge,get,set}
```

-h

вывод справки

-v

вывод на консоль логов в процессе выполнения утилиты.

merge

объединение нескольких конфигурационных файлов

```
nt-config-tool merge [-h] src dest
```

-h

вывод справки

src

конфигурационный файл

dest

конфигурационный файл, который объединяется с *src*

get

получение данных из конфигурационного файла по ключам

```
nt-config-tool get [-h] cfg key
```

-h

вывод справки

cfg

конфигурационный файл

key

перечень ключей из конфигурационного файла (в качестве разделителя ".")

set

установка значений в конфигурационном файле по ключам

```
nt-config-tool set [-h] [-t {int,str,float,list}] cfg key value
```

-h

вывод справки

-t {int,str,float,list}

тип значений, устанавливаемых по соответствующим ключам

cfg

конфигурационный файл

key

перечень ключей из конфигурационного файла (в качестве разделителя ".")

value

значение по ключу

nt-data-backup

Позволяет сохранить данные пользовательских сессий к целевым системам в архив *ARCHIVE*, по умолчанию резервные копии данных размещаются в директории `/opt/skdpu-nt-data/backup/backup-host_name-YYYYMMddhhmmss/`

```
nt-data-backup [-h] [-c CONFIG] [-v] [-n] [-z] -r [-a ARCHIVE]
```

-h

вывод справки

-c CONFIG

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты

-n

только вывод статистики

-z

использовать `gzip` для сжатия

-r

без указания этого параметра, действия выполняться не будут

-a ARCHIVE

имя архива.

nt-data-restore

Позволяет разместить ранее сделанную резервную копию данных сессий из архива *ARCHIVE* в хранилище системы

```
nt-data-restore [-h] [-c CONFIG] [-v] [-n] [-z] -r [-a ARCHIVE] [-b]
```

-h

вывод справки

-c CONFIG

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты

-n

только вывод статистики

-z

использовать `gzip` для сжатия

-r

без указания этого параметра, действия выполняться не будут

-a ARCHIVE

путь и имя архива.

-b

загрузка данных в поточном режиме

nt-data-rotate

Утилита позволяет сохранять и удалять старые данные из архива системы, начиная с самых старых, в соответствии с параметрами политики ротации, по умолчанию резервные копии данных размещаются в директории `/opt/skdpu-nt-data/backup/archive-host_name-YYYYMMddhhmmss.tgz`.

```
nt-data-rotate [-h] [-c CONFIG] [-v] [-n] [-z] -r [-a ARCHIVE] [-x]
                [-k] [--move-storage] [-d DATE | -m MONTHS]
```

-h

вывод справки

-c CONFIG

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты

-n

только вывод статистики

-z

использовать `gzip` для сжатия

-r

без указания этого параметра, действия выполняться не будут

-x

удалять данные, которые были ротированы

--move-storage

использовать перемещение объектов, а не копирование

-k

выполнить очистку промежуточных результатов через фоновую задачу

-a ARCHIVE

путь и имя архива

-d DATE (YYYY-MM-DD)

ротировать данные, старше указанной даты

-m MONTHS

оставить в системе данные за указанное число месяцев.

nt-db-reset

Утилита для сброса системы к заводским настройкам. Эта утилита позволяет сбросить базу данных, восстановить исходное состояние системы, удалив все данные из хранилища и базы данных

```
nt-db-reset [-c CONFIG] [-h] -f [-r]
```

-c CONFIG

выбор конфигурационного файла *CONFIG*

- f**
без этого ключа удаление данных произведено не будет
- r**
очистить внутренние очереди системы
- h**
вывод справки.

nt-delete-reports

Утилита для регулярного удаления старых пользовательских отчетов. Выполняется по расписанию и использует системные настройки хранения отчетов.

```
nt-delete-reports [-h] -r [-c CONFIG] [-v]
```

- h**
вывод справки
- r**
без этого ключа удаление производиться не будет
- c CONFIG**
выбор конфигурационного файла *CONFIG*
- v**
вывод на консоль логов в процессе выполнения утилиты

nt-gen-cert

Утилита для создания самоверяющего сертификата веб-сервера СКДПУ НТ. Для работы системе требуется сертификат веб-сервера в `/opt/skdpu-nt/var/ssl`. Во время установки эта утилита используется для создания самоверяющего сертификата. Кроме того, системный оператор может скопировать в этот каталог постоянный сертификат веб-сервера по умолчанию, выданный уполномоченным центром сертификации

```
nt-gen-cert [-t DIR] [-o FILE]
```

- t DIR**
целевая директория, по умолчанию `/opt/skdpu-nt/var/ssl`
- o FILE**
конфигурационный файл *openssl*.

nt-indexctl

Утилита для работы с полнотекстовым индексом.

```
nt-indexctl [-h] flush
```

- h**
вывод справки

flush

сбросить накопленный процессом индексации кэш принудительно.

nt-integrity-check

Инструмент контроля целостности исполняемых файлов СКДПУ НТ. Обычно выполняется как фоновый процесс. Если есть изменения, будет присутствовать предупреждение для оператора.

```
nt-integrity-check [-h] [-v] [-d DB_PATH] [-b BLOCK_SIZE]
                  [-e ERROR_PATH] {create,verify,reset}
```

-h

вывод справки

-v

вывод на консоль логов в процессе выполнения утилиты.

-d DB_PATH

путь к базе контрольных сумм

-b BLOCK_SIZE

размер буфера в байтах

-e ERROR_PATH

путь к файлу с описанием возникающих ошибок

create

создание контрольных сумм

```
nt-integrity-check create [-h] [-r SET_ROOT] [-w WORK_DIR] -p PATH
```

-h

вывод справки

-r SET_ROOT

корневой путь к контролируемым файлам

-w WORK_DIR

изменить рабочую директорию

-p PATH

путь к контролируемым файлам (перечисление через запятую)

verify

проверка контрольных сумм

```
nt-integrity-check verify [-h] [-n] [-a] [-s SOURCE]
```

-h

вывод справки

-n

не проверять целостность контролируемых файлов

-a

записывать ошибки целостности в файл *ERROR_PATH*

-s SOURCE

путь к контролируемым неcompiled файлам (перечисление через запятую)

reset

сброс имеющихся предупреждений.

```
nt-integrity-check reset [-h]
```

-h

вывод справки

nt-listenerctl

Инструмент для управления приемом входящих данных

```
nt-listenerctl [-h] [-s] -e|-d
```

-h

вывод справки

-s

получить статус получения данных

-e

начать прием данных

-d

закончить прием данных

nt-network-filter

Управление сетевыми настройками СКДПУ НТ

```
nt-network-filter enable|disable|status
```

enable

применить настройки

disable

отключить настройки

status

узнать статус

nt-oem

Переключает темы оформления интерфейса

```
nt-oem [-h] enable|disable
```

-h

вывод справки

enable

активировать тему

disable

отключить тему.

nt-profile

Утилита позволяет «забыть» профиль указанной персоны в рамках системы. В результате, накопленное содержимое профиля будет из системы безвозвратно удалено. Новые данные от этого пользователя приведут к созданию профиля заново.

```
nt-profile [-h] [-c CONFIG] [-v] {forget}
```

-h

вывод справки

-c CONFIG

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты.

forget

удаление персоны

```
nt-profile forget [-h] pid [pid ...]
```

-h

контекстная помощь

pid

идентификатор персоны

nt-restore-backup

Утилита для восстановления настроек СКДПУ НТ

```
nt-restore-backup [-h] -r [-c CONFIG]
```

-h

вывод справки

-r

без этого ключа восстановление производиться не будет

-c CONFIG

выбор конфигурационного файла *CONFIG*

nt-restore-default-admin

Восстанавливает пароль по умолчанию для учетной записи *admin*. Эта утилита обеспечивает восстановление доступа к веб-интерфейсу при утере или истечении срока действия пароля администратора

```
nt-restore-default-admin [-h] -f [-p PASSWORD] [-c CONFIG] [-v]
```

-h

вывод справки

-f

флаг обязательной смены пароля

-p *PASSWORD*

задание нового пароля *PASSWORD*

-c *CONFIG*

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты.

nt-restore-settings

Утилита для восстановления настроек СКДПУ НТ из указанного архива *archive_name*

```
nt-restore-settings [-h] [-v] [-p PATH] [-f] archive_name
```

-h

вывод справки

-v

вывод на консоль логов в процессе выполнения утилиты

-p *PATH*

путь *PATH* для распаковки архива

-f

флаг замены существующих файлов

archive_name

имя архива.

nt-run-report

Утилита, запускающая составление отчетов. Эта утилита обычно запускается автоматически, и ее не следует запускать вручную.

```
nt-run-report [-h] -r [-c CONFIG] [-v]
```

-h

вывод справки

-r

без указания этого параметра, действия выполняться не будут

-c *CONFIG*

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты

nt-run-script

Утилита, запускающая необходимые команды в рамках фонового процесса. Эта утилита обычно запускается автоматически, и ее не следует запускать вручную.

```
nt-run-script [-h] -r RUN [-c CONFIG] [-v]
```

-h

вывод справки

-r RUN

выполнить команду *RUN*

-c CONFIG

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты

nt-status

Утилита для получения информации о состоянии системы. Утилита позволяет быстро получить доступ к информации о состоянии системы. Утилита может запускаться с минимальными привилегиями.

```
nt-status [-h] [--format {text,json}] [-c CONFIG]
```

-h

вывод справки

-format {text,json}

вывод в указанном формате, text или json. По умолчанию text.

-c CONFIG

выбор конфигурационного файла *CONFIG*

nt-storagectl

Утилита управления данными в хранилище.

```
nt-storagectl [-h] [-v] [-p VOLUME_PATH] {verify,rebuild,rungc,dump}
```

-h

вывод справки

-v

вывод на консоль логов в процессе выполнения утилиты

-p VOLUME_PATH

путь к хранилищу данных

verify

проверка целостности данных

```
nt-storagectl verify [-h] [-t] [-o OUTPUT] [-m {text,html,csv}]
```

```

[-x {OPEN, MISSING_FILE, BAD_CHECKSUM,
NO_CHECKSUM,
GC_ELIGIBLE}]
NO_DB_RECORD, NO_STORAGE_DATA,
[-r] (-s SESSION | -a)

```

-h

вывод справки

-t

вывод сессий только с полным набором данных

-o OUTPUTвыходной файл *OUTPUT* с отчетом**-m {text,html,csv}**

выходной формат отчета

-x {OPEN, MISSING_FILE, BAD_CHECKSUM, NO_CHECKSUM, NO_DB_RECORD, NO_STORAGE_DATA, GC_ELIGIBLE}

исключить различные ошибки из рассмотрения

-r

восстановить поврежденные сессии

-s SESSIONпроверка указанной сессии *SESSION***-a**

проверка всего объема хранилища

rebuild

восстановление поврежденных метаданных

```
nt-storagectl rebuild [-h]
```

-h

вывод справки

rungc

финализирование завершившихся сессий

```
nt-storagectl rungc [-h] [-f]
```

-h

вывод справки

-f

запустить сборщик мусора

dump

вывод свойств указанной сессии.

```
nt-storagectl dump [-h] sid
```

-h

вывод справки

sid

идентификатор сессии

nt-support-bundle

Генерирует файл с архивом журналов и настроек СКДПУ НТ для передачи в службу технической поддержки

```
nt-support-bundle [-h] [-v] [-u USER] target
```

-h

вывод справки

-v

вывод на консоль логов в процессе выполнения утилиты

-u *USER*

информация о пользователе *USER*

target

путь к директории, куда будут помещены все необходимые материалы.

nt-system-metrics

Выполняется автоматически по расписанию и записывает сведения об использовании ресурсов системы.

```
nt-system-metrics [-h] -r [-c CONFIG] [-v]
```

-h

вывод справки

-r

без указания ключа, данные считываться не будут.

-c *CONFIG*

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты

nt-tlupdate

Утилита для обновления уровня доверия. Утилита последовательно увеличивает уровень доверия для всех авторизованных лиц. Запускается автоматически, обычно не запускается вручную.

```
nt-tlupdate [-h] -u [-c CONFIG] [-v]
```

-h

вывод справки

-u

произвести обновление уровня доверия

-c *CONFIG*

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты

nt-update-domain-data

Утилита обновляет данные персон из подключенных внешних домен-контроллеров. Запускается регулярно по расписанию.

```
nt-update-domain-data [-h] -r [-c CONFIG] [-v]
```

-h

вывод справки

-r

без указания ключа, данные считываться не будут.

-c CONFIG

выбор конфигурационного файла *CONFIG*

-v

вывод на консоль логов в процессе выполнения утилиты

nt-version

Утилита выводит информацию о сборке СКДПУ НТ.

```
nt-version [-h] [-v] [-b] [-f] [-c CONFIG]
```

-h

вывод справки

-v

вывод на консоль логов в процессе выполнения утилиты

-b

вывод на консоль даты сборки

-f

вывод на консоль полной информации о сборке

-c CONFIG

выбор конфигурационного файла *CONFIG*

nt-volume-check

Утилита проверяет объекты хранения на предмет целостности данных и связей. Эквивалент `nt-storagectl verify`.

```
nt-volume-check
```

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

API	Application Programming Interface — описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой.
CEF	Common Event Format разработан для унификации событий от разных технических средств. В качестве транспортного механизма CEF использует стандарт syslog-сообщения.
CPU	Central Processing Unit дословно (центральное обрабатывающее устройство) — электронный блок либо интегральная схема, исполняющая машинные инструкции (код программ), главная часть аппаратного обеспечения компьютера или программируемого логического контроллера.
HTTP	HyperText Transfer Protocol — протокол передачи гипертекста.
ISO	International Organization for Standardization — международная организация, занимающаяся выпуском стандартов.
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
NTLM	NT LAN Manager — протокол сетевой аутентификации, разработанный фирмой Microsoft для Windows NT.
POSIX	Portable Operating System Interface (переносимый интерфейс операционных систем) — набор стандартов, описывающих интерфейсы между операционной системой и прикладной программой (системный API), библиотеку языка C и набор приложений и их интерфейсов.
RAM	Random Access Memory — один из видов памяти компьютера, позволяющий одновременно получить доступ к любой ячейке (всегда за одно и то же время, вне зависимости от расположения) по её адресу на чтение или запись.
RFC	Remote Function Call — это функция, которая может вызвать и запустить на выполнение функциональный модуль, расположенный в другой системе.
RLOGIN	Remote LOGIN — удалённый вход в систему.

RSA	RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.
SASL	Simple Authentication and Security Layer (простой уровень аутентификации и безопасности) — это фреймворк (каркас) для предоставления аутентификации и защиты данных в протоколах на основе соединений.
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.
SIEM	Security information and event management — объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) - управление информацией о безопасности, и SEM (Security event management) - управление событиями безопасности.
SMTP	Simple Mail Transfer Protocol (простой протокол передачи почты) — широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.
SMTPS	Simple Mail Transfer Protocol Secure — это метод защиты SMTP с использованием безопасности транспортного уровня. Он предназначен для обеспечения аутентификации партнеров по общению, а также целостности и конфиденциальности данных.
SSH	Secure SHell (безопасная оболочка) — протокол защищенной передачи данных.
TCP	Transmission Control Protocol (протокол управления передачей) — один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета.

TELNET	TErminaL NETwork — сетевой протокол для реализации текстового интерфейса по сети (при помощи транспорта TCP).
TLS	Transport Layer Security — протокол защиты транспортного уровня
UDP	User Datagram Protocol (протокол пользовательских датаграмм) — один из ключевых элементов набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных.
URL	Uniform Resource Locator (унифицированный указатель ресурса) — система унифицированных адресов электронных ресурсов.
АРМ	Автоматизированное рабочее место
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 – Форма ввода логина и пароля.....	11
Рисунок 2 – Ошибка входа.....	12
Рисунок 3 – Интерфейс СКДПУ НТ.....	13
Рисунок 4 – Раздел Права доступа Пользователи.....	16
Рисунок 5 – Раздел Права доступа Роли.....	28
Рисунок 6 – Раздел Права доступа Ограничения доступа к данным.....	31
Рисунок 7 – Настройки детекторов аномалий.....	41
Рисунок 8 – Уровни доверия.....	46
Рисунок 9 – Настройка интеграции с SIEM.....	57
Рисунок 10 – СКДПУ версии 7.....	58
Рисунок 11 – Раздел Настройки Настройки LDAP.....	68
Рисунок 12 – Раздел Настройки Конфигурация журналирования.....	77
Рисунок 13 – Раздел Отчеты Журнал авторизаций.....	83
Рисунок 14 – Раздел Диагностика.....	86
Рисунок 15 – Статистика компонента collectd.....	87
Рисунок 16 – Статус приемника.....	94

ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1 – Минимальные характеристики аппаратно-программного обеспечения АРМ пользователя СКДПУ НТ.....	9
Таблица 2 – Права доступа к разделам веб-интерфейса СКДПУ НТ.....	21
Таблица 3 – Настройка прав профилей.....	22
Таблица 4 – Доступные для управления сервисы.....	86

