Руководство администратора системы Infozorok

ООО «ИБ-ИННОВАЦИИ» 2025

Содержание

Перечень условных обозначений и сокращений	3
1.Возможности системы	4
2. Установка системы	5
2.1.Системные требования	5
2.2.Подготовка	5
2.3.Генерация ключей шифрования	7
2.4. Установка сервера	7
2.5.Установка агента	7
2.6.Активация агента	8
3.Администрирование системы	9
3.1.Общие принципы	9
3.2.Настройка интеграций	.12
3.3.Настройка алертов	. 16
3.4.Настройка автоматизации	. 19
3.5. Регистрация пользователей и разграничение прав лоступа	.21
4. Устранение неисправностей	.23

Перечень условных обозначений и сокращений

Модуль	Логическое объединение данных в системе в соответствии с выполняемым функционалом
Коллекция	Единица организации данных в системе, аналог таблицы в базе данных
Объект коллекции	Запись в коллекции системы, аналог строки в таблице базы данных
Объединяющая коллекция	Особый тип коллекции, которая связывает коллекции- источники по общему признаку и отображает информацию в едином интерфейсе, аналог сводной таблицы

1.Возможности системы

Система информационной безопасности InfoZorok - это программное решение, которое интегрирует несколько функций безопасности в единую платформу.

Выполняет такие задачи как инвентаризация и управление ИТ-активами, контроль конфигураций, управление событиями, а так же централизованный сбор и анализ данных за счет интеграции с другими системами информационной безопасности.



Гибкая структура решения позволяет оперативно добавлять новый функционал. Имеет единую консоль, что обеспечивает централизованной контроль различных аспектов безопасности. Система предоставляет возможность улучшить защиту за счет комплексного подхода к безопасности. Это помогает снизить сложность управления безопасностью и повысить эффективность обнаружения и реагирования на угрозы.

2.Установка системы

Администратор системы должен обладать базовыми знаниями:

- технологии контейнеризации
- программирования на языке python
- язык запросов sql (postgresql)

Перед началом работы рекомендуется ознакомиться с Инструкцией пользователя.

Система состоит из трех компонентов:

1.Сервер - содержит веб-сервер и базу данных

2.Агент - содержит службу с помощью которой осуществляется подключение к источникам информации, сбор этой информации и ее обработка в базе данных

3.Сервер лицензий (на стороне вендора) - подтверждение запросов на выпуск контрольного значения лицензии

2.1.Системные требования

Infozorok Server:

OS - Ubuntu 24.10 Server RAM - 4Gb Storage - 50Gb **Infozorok Agent:** OS - Ubuntu 24.10 Server RAM - 4Gb Storage - 50Gb

Для корректной установки необходимо чтобы оба сервера имели записи в DNS, корректно настроенную службу времени NTP и установленную последнюю версию Docker Swarm и PSQL.

Допускается установка сервера и агента на одном хосте.

2.2.Подготовка

Для работы системы на серверах необходимо установить Docker Swarm и PSQL. Для этого выполните следующие команды: curl -fsSL https://get.docker.com -o get-docker.sh sudo sh get-docker.sh sudo usermod -aG docker \$USER перезагрузите сервер - sudo reboot now docker swarm init --advertise-addr <ip-адрес сервера в локальной сети> sudo apt install -y postgresql-client

Распакуйте полученный от вендора дистрибутив в домашний каталог с помощью команды от sudo:

sudo tar -xzf iz.tar.gz

Каталог дистрибутива имеет следующую структуру:



Каждый корневой каталог относится к компоненту системы:

1.izserver - сервер Infozorok (веб-сервер и база данных)

2.izagent - агент InfoZorok

3.izca - ключи СА, на основе которых сформированы ключи для веб-сервера (TLS)

В корне находится скрипт для генерации всех необходимых ключей — keys_generate.sh.

Установка состоит из четырех этапов:

1. Генерация ключей (этот этап можно пропустить и воспользоваться для ознакомления с системой уже сгенерированными тестовыми ключами)

2. Установка сервера

Установка агента
 Активация продукта

2.3.Генерация ключей шифрования

1.Перейдите в каталог iz и выполните команду

cd ~/iz

./keys_generate.sh

введите FQDN имя сервера, на который будет установлена система InfoZorok

В результате будут сгенерированы криптографические ключи агента, сервера, локального центра сертификации и помещены в каталоги keys соответствующего дистрибутива (izagent, izserver, izca).

2.Для обеспечения безопасности переместите сгенерированные ключи локального удостоверяющего центра (каталог iz/izca) во внешнее защищенное хранилище.

2.4.Установка сервера

1.Перейдите в каталог iz/izserver и выполните команду

cd ~/iz/izserver

./izserver_install.sh

введите FQDN имя сервера InfoZorok. В ходе установки необходимо будет придумать пароль для сервисной учетной записи базы данных системы.

2.Проверьте корректность работы стека Infozorok командой

docker service ls

все сервисы должны быть запущены (статус "1/1")

3.Выполните вход в интерфейс сервера InfoZorok (https://<FQDN сервера, который вы указывали при установке>). Начальный логин - admin@admin.com пароль - d@faultp#ssword 4.Смените логин и пароль администратора в профиле (в левом нижнем углу), поля Email и Password.

5.Перейдите в меню System->Settings и заполните полученные от вендора лицензионный ключ и срок его действия в двойных кавычках ("license_key" и "license_expiry" в формате ГГГГ-ММ-ДД).

2.5.Установка агента

1.Перенесите каталог с дистрибутивом агента (iz/izagent) на нужный сервер и выполните команду

cd ~/iz/izagent

./izagent_install.sh

введите FQDN имя сервера InfoZorok, уровень логирования (нажмите ENTER для установки рекомендуемого значения) и интервал работы агента (нажмите ENTER для установки рекомендуемого значения).

2.Проверьте корректность работы стека агента командой docker service ls

2.6.Активация агента

1.Выполните вход в интерфейс сервера InfoZorok

Для доступа к интерфейсу системы необходимо перейти по адресу, где опубликован webсервер системы (https://<aдрес cepвepa>/admin/login). Начальный логин - admin@admin.com пароль - d@faultp#ssword

InfoZorok Application	
Sign In	
Email	
	©
Sign In	Forgot Password

2.В меню Hactpoйки->Settings, скопируйте сертификат и запрос на контрольное значение ("license_certificate" и "license_control_value_request") и отправьте их вендору.

Примечание. На стороне вендора. После получения от клиента запроса на контрольное значение и сгенерированный им сертификат, администратор на стороне вендора запускает утилиту infozorok_distr/vendor/izlserver/generate-cv.

Далее последовательно вводит, без двойных кавычек:

- пароль секретного ключа (secret key password)

- control value request
- license certificate
- license key value

Проверяет содержимое запроса, генерирует контрольное значение (Control value) и отправляет клиенту

3.После получения от вендора контрольного значения, coxpaните его в "license_control_value". 4.Перейдите в меню Настройки->Agent, найдите вновь созданного агента (в поле Sys Job Id будет 0 items). Назначьте новому агенту тестовую задачу, например test_job1, которая будет записывать строку "agent1" в коллекцию test1.

5.Перейдите в главном меню в Test->test1, подождите период обновления (30 секунд) и убедитесь, что новые значения добавляются.

6.Логи работы системы и возможные ошибки можно посмотреть в журнале, пункт Event главного меню.

3. Администрирование системы

3.1.Общие принципы

Администрирование системы осуществляется в модуле Настройки.



Настройки системы задаются в коллекции Setting, например SMTP-сервер для отправки алертов, параметры подключения к серверам HR-систем, LDAP-каталогу и др. Для добавления или изменения настройки необходимо выбрать значение с соответствующим именем и изменить значение в виде JSON-строки.

1	InfoZorok	 Settings Редактирование элемента в Settings
Ø		
3	🚉 Кадры	Name sys_smtp
*	 Активы Учетные записи 	> Value
\$	Инфосистемы Программы Погоницита	<pre> 1 { 2 "smtp_server": "smtp.yandex.ru", 3 "smtp_port": "465", </pre>
	 Документы Мнциденты Задачи 	<pre>4 "smtp_ssl": 1, 5 "smtp_usr": "test@yandex.ru", 6 "smtp_admin_mail": "test@yandex.ru", 7 "smtp_admin_mail": "test@yandex.ru"</pre>
	Hастройки	<pre>% *smtp_header*: *<head><meta charset="utf-8"/></head><body>*, % *smtp_footer*: *</body>* 10 }</pre>
	Group	System Description
	Settings	
	 События Тест Тест 	

Пароли, API-ключи и другая секретная информация хранится в системе в зашифрованном на ключах агента виде, в коллекции Secret. Чтобы добавить секрет, необходимо выбрать значение с соответствующим именем и изменить значение.

r	InfoZorok	 Secret Редактирование элемента в Secret
Θ		
8	281 Кадры	Name
-	🔚 Склад	smtp_password
	📋 Активы	
24	🧧 Учетные записи	Value
	Инфосистемы	
1	🔲 Программы	
	[👌 Документы	
	\land Инциденты	
	🖸 Задачи	
	🔀 Настройки	
	e Agent	
	dol 🗎	
	😑 Step	
	🤤 Group	
	Settings	
	Secret	
	🔄 События	
	🛅 Тест	
	E Test1	

Сбор и обработка информации из внешних систем выполняется агентами, на которых настраиваются соответствующие инструкции и расписание их выполнения.

Принцип работы агентов следующий. Создается работа (Job), которая назначается агенту. В работе указывается расписание ее запуска. В состав работы входит один или несколько шагов (Step), в параметрах которых указываются:

- тип шага (update — интеграция с внешним источником и загрузка данных в систему, event

— мониторинг на предмет выявления несоответствия и отправка алерта)

- инструкции и что именно необходимо сделать.

Информация о зарегистрированных агента находится в коллекции Agent и содержит:

- имя агента
- серийный номер
- ссылки на работы, выполняемые агентом

K	InfoZorok	Agent Редактирование элемента в Agent	
$\widehat{\mathbf{O}}$			
8	<u>:≗</u> : Кадры	Name	
	🔚 Склад	iz-agent01	
*	Учетные записи	Serialnumber	
ŝ	 Инфосистемы Программы 		
	Документы	Svs Job ID	
	🖸 Задачи	event_send	
	🔀 Настройки	ldap_update_full	
	job	pinger_event	
	Step	asset_update_full	
	Settings	account_update_full	
	Secret	asset_event_new	
	События Тест	test_job1	
	E Test1	person_update_full	

Работы настраиваются в коллекции Job. Каждая работа имеет несколько параметров: - имя

- тип запуска (interval — раз в период, date - по наступлению даты, once — однократно, on start — при запуске агента)

- параметры запуска (если interval — указываются часы/минуты/секунды, если дата — в формате «ГГГГ-ММ-ДД ЧЧ:ММ:СС»)

r	InfoZorok		 Редактирование элек 	мента в	в Јођ	
Θ						
8	281 Кадры		Name		Active	
	🚰 Склад		ldap_update_full		Включено	
	📕 Активы					
*	Учетные записи		Sys Agent ID		Sys Step ID	
ស៊ី	Инфосистемы		iz-agent01	<i>i</i> ⁰ ×	= Idap_load_full	
~	📑 Программы					
	Документы				= Idap_update_full	
	Document Employ	ee				
	🗸 Инциденты				Создать	
	🖸 Задачи				Добавить существующий	
	🔀 Настройки					
	Agent		Trigger		Trigger Params	
	job		interval			
	😑 Step				2 "seconds": 60 3 }	
	Group					
	Settings					
	Secret					
	События		Description			
	E Test1		besenption			
	e losti					

Шаги с инструкциями выполнения указываются в коллекции Step (Шаг).

Step имеет следующие параметры и инструкции:

- ИМЯ

- sys job id работа, в рамках которой выполняется шаг
- тип (update загрузка данных/обновление, event задача мониторинга)
- language язык, на котором будут написаны инструкции (python/sql)
- python result var имя коллекции, которая будет содержать данные по выявленным событиям, если выбран тип event и язык python
- command инструкции для выполнения

r	InfoZorok	 ^{Step} Редактирование элемента в Step
Ŷ		
	<u>:2:</u> Кадры >	Name
C	🔚 Склад >	ldap_load_full
*	Учетные записи >	Sys Job ID
	 (i) Инфосистемы) Программы 	= Idap_update_full
	 Документы Document 	Создать Добавить существующий
	Document Employee Мнциденты >	Type Language
	🔄 Задачи 💦 👌	update ~ python ~
	 Настройки Agent Job Step Group 	Python Result Var
	Settings	Command
	😑 Secret 🔄 События События Стест У 🖨 Test1	1 import ldap 2 import struct 3 import uuid 4 import datetime 5 import pytz

Для отправки алертов через электронную почту необходимо создать группу рассылки в коллекции Group и добавить в группу аккаунт (из коллекции Account).

3.2.Настройка интеграций

Приведем пример настройки интеграции с каталогом LDAP, для получения информации о пользователях.

1.Добавляем в коллекцию Setting параметры подключения к контроллеру домена, откуда будут выгружаться данные:

÷	Sett Pe	^{ілдз} 2дактирование элеме	нта в Settings	
Name				
lp_se	erver			
Value				
		{		
		"host": "192.168.57.2",		
		"port": "389",		
		"lg": "s.iz.ldap",		
		"base": "DC=ab.DC=loc"		
		}		

2.В коллекции Secret добавляем пароль для подключения к LDAP:

¢	^{Secret} Редактирование элемента в Secret
Name	
ldap_	password
Value	
••••	

3. Настраиваем Job:

- name: ldap_update_full

- active: выключено
- agent: выбираем агент, который будет выполнять работу

- sys step id: ссылка на step-ы, которые загружают данные об учетных записях пользователей из LDAP и обновляют данные базе данных (создание описано ниже)

- trigger: interval (периодами)
- trigger params: { seconds: 60 } (работа будет запускаться раз в минуту)

K	InfoZorok	🔶 🧖 Редактирование элемента	в Јор
\bigcirc	Поиск коллекций		
90	🚓 Кадры 🗸 🗸	Name	Active
	 Person Employee 	ldap_update_full	Включено
*	Structure Anketa	Sys Agent ID	Sys Step ID
<u>ت</u> ې	😂 Spravka	iz-agent01 🖉 ×	= Idap_load_full
	Absence		
	🔚 Склад 🛛 🗸		= Idap_update_full
	Stock >		
	🗧 Активы 🗸 🗸		Создать
	😂 Asset 🛛 🔶		Добавить существующий
	🧧 Учетные записи \vee		
	😂 Account 💦 >	Trigger	Trigger Params
	🚺 Инфосистемы 🗸 🗸		
	😑 Infosystem	interval 🗸 🗸	
	📑 Программы 🗸 🗸		
	E KSC Software		
	🗋 Документы 🗸 🗸		
	Document		
	1 Document Emplo	Description	
	🔺 Инциденты 🗸 🗸		

4. Настраиваем Step выгрузки данных из LDAP:

- name: ldap_load_full

- sys job id: в рамках какой работы будет выполняться step — ldap_update_full

- type: update
- language: python (язык программирования, на котором описана инструкция)

- command: сама инструкция на языке python, которая получает параметры сервера и секрет (пароль) для подключения, подключается к LDAP и загружает данные в виде списка, сохраняет список во временную таблицу (полный листинг инструкции алерта можно посмотреть в уже настроенном шаге)

r	InfoZorok	 Step Федактирование элемента в Step 	
Ŷ			
	:2: Кадры	V Name	
	Person	Idap_load_full	
	Employee		
*	Anketa	Sys Job ID	
	😑 Spravka	= ldap_update_full	
	E Absence		
	🔚 Склад	Создать Добавить существующий	
	Stock	>	
	📋 Активы	V Type Language	
	🖨 Asset	> update > python >	
	🧧 Учетные записи	• • • • • • • • • • • • •	
	Account	> Duthon Result Var	
	🚺 Инфосистемы		
	闫 Infosystem		
	🔲 Программы	v	
	😑 KSC Software	Command	
	[Документы	<pre>> 1 import ldap</pre>	
	😑 Document	2 import struct	

5.Настраиваем Step для обновления данных в базе:

- name: ldap_update_full
- sys job id: в рамках какой работы будет выполняться step ldap_update_full
- type: update
- language: sql (язык программирования, на котором описана инструкция)

- command: инструкция на языке sql, которая делает копию таблицы для выявления изменений, используя временную таблицу, полученную на предыдущем шаге, обновляет целевую таблицу - помечает удаленные объекты, обновляет существующие, вставляет новые (полный листинг инструкции алерта можно посмотреть в уже настроенном шаге)

K	InfoZorok	 ^{Step} Редактирование элемента в Step
Ø		
න	:2: Кадры	Name
	Person	Idap_update_full
*	Structure	Sys Job ID
袋	Spravka	= Idap_update_full
	😑 Absence	
	🔚 Склад	Создать Добавить существующий
	Stock	> · · · · · · · · · · · · · · · · · · ·
	📋 Активы	Type Language
	🖨 Asset	> update y sql y
	🧧 Учетные записи	
	😑 Account	Duthon Bosult Var
	🚺 Инфосистемы	
	闫 Infosystem	
	🔲 Программы	
	😑 KSC Software	Command
	🗋 Документы	1 ldap_user
	😑 Document	
	🔨 Document Emp	IO 4 SELECT •
	\land Инциденты	✓ 5 INTO lp_user_last
	😑 Incident	> 6 FROM Lp_user;
	💟 Задачи	8 UPDATE lp_user

- 6.Активируем работу с помощью параметра «active» Job-а.
- 7. Проверяем в системном журнале, что работа запустилась и ошибок нет:

Ę	контент Собы	тия 🛛			
	ID	When Created =	Information	Message	Sent
	2	28 апреля 2025 г. 18:56	Daemon	Message: Start step "Idap_update_full"	×

3.3.Настройка алертов

Приведем пример настройки алерта для выявления новых учетных записей пользователей в каталоге LDAP.

1. Настраиваем системную группу для отправки алертов со следующими параметрами:

- name: «group_ldap_user_new»

- an account id: список учетных записей для отправки

- sys step id mailto: ссылка на step, который выявляет новые учетные записи в LDAP (создание описано ниже)

	InfoZorok		 Сточир Редактирование элемента в Group 	
Θ		Ĩ		
8	28: Кадры	~	Name	
	Person		group_Idap_user_new	
*	Structure		· An Account ID	
ŝ	😂 Spravka		🛛 nnikolaev@ab.loc 🛛 🕹	
	Absence			
	拱 Склад	~	Добавить существующий	
	Stock	>		
	📃 Активы	~	Sys Step ID Mailto	
	😂 Asset	>	ldap_user_new	
	Учетные записи	~	-	\square
	Account	>	Создать Добавить существующий	
	() Инфосистемы	~		

2.Настраиваем Job:

- name: ldap_user_new
- active: выключено
- agent: выбираем агент, который будет выполнять работу

- sys step id: ссылка на step, который выявляет новые учетные записи в LDAP (создание описано ниже)

- trigger: interval (периодами)
- trigger params: { seconds: 60 }

Пример создания работы:

K	InfoZorok	 Редактирование элемента 	в Јор
Θ			
ୁ	<u>₂≗</u> Кадры	Name	Active
	Employee	idap_user_new	выючено
*	Structure	Sys Agent ID	Sys Step ID
1	😑 Spravka	iz-agent01 🧷 🗡	 Нет элементов
	Absence		Создать
	Склад		
	Учетные записи		Добавить существующий
	 Инфосистемы 	Trigger	Triager Darame
	📑 Программы	1113721	
	🗋 Документы	interval	
	\land Инциденты		
	🗹 Задачи		
	🔀 Настройки		
	Agent		
	Job	Description	
	Group	Работа для обнаружения новых учетных записей	пользователей в LDAP
	Settings		
	Secret		
	😑 Secret 🗐 События		

3.Настраиваем Step:

- name: ldap_user_new

- sys job id: в рамках какой работы будет выполняться step — ldap_user_new

- type: event
- language: sql

- command: инструкция на языке sql, которая выводит количество новых строк с момента последнего обновления

- attachment command: инструкция на языке sql, которая выводит сами новые строки добавленные в базу с момента последнего обновления

- information template: заголовок email-сообщения - «LDAPUSER Обнаружена новая учетная запись пользователя»

- message template: шаблон email-сообщения в котором используется плейсхолдер из command - «В домене обнаружено {{cnt}} новых учетных записей пользователей»

- need sending: требуется отправка, или алерт будет просто записываться в системный журнал

- sending type: каким способом будет отправляться уведомление - «mail»

- insert attachment: как будет добавлена информация из attachment command (в тело письма в виде таблицы, или файлом вложения) - «body»

- sys group id mailto: системная группа, на учетные записи которой будет отправляться алерт - «group_ldap_user_new»

Image: Second state Name Image: Second state Second state	K	InfoZorok	 Втер Редактирование элемента в Step 	
Image: Angle image: Free and im	\Diamond	Поиск коллекций		
International interpreter i		<u>:8</u> : Кадры 🗸 🗸	Name	
Browsee B		Person	Idap_user_new	
Systake Systake		Employee		
Status <		Structure	Sys Job ID	
Second Contact <th></th> <th>Anketa</th> <th>= Idan user new</th> <th>π</th>		Anketa	= Idan user new	π
Image: Constant in the second of the seco		Absence		
Image: State in the status is interval in the state in the state is interval in the state is inthe state is interval in the state is interva		🔚 Склад 🗸	Создать Добавить существующий	
Advent Werness stature Advocatination Werness stature Advocatination Python Result Var Command I Stature Command I			Type Language	
Image of the second is a second in the second is a second in the second is a second in the second is a second is second is second is a second is a second is a second i		Asset		
Account Index certifier of the document of the second of the		🧧 Учетные записи 🗸	event Sql V	
<pre>Python Result Var hotosystem hotosystem Regression KGC Software Command iffict cit FRM { Decomment Employ Autochment Employ Software Advance Software Advance Software Advance Software Advance Software Account Employ Software Advance Software Account Employ Account Emplo</pre>		Account >		
Protocytame Command StillC1 cet F608 { StillC1 cet F608 { StillC1 cet F608 { StillC1 cet F608 { StillC1 cet F608 { StillC1 cet F608 { StillC1 cet F608 { StillC1 cet F608 { StillC1 cet F608 { StillC1 cet F608 { StillC1 cet F608 {		🕕 Инфосистемы 🗸 🗸	Python Result Var	
Importantial Command Importantial Importantial		😂 Infosystem		
Account of the second of		🔲 Программы 🗸		
Statist ext Replet Statist control (1) Statist control (1) Statist COMPT(1)::::::::::::::::::::::::::::::::::::		KSC Software	Command	
Document Employ Multiplement Document Employ Multiplement			1 SELECT cnt FROM (2 SELECT COUNT(lu.id) as cnt	
Maugaanau Site to 10 Michael (p_seer EXCEPT SELECT 1d 960% (p_user_last) Site to 10 Michael (p_seer EXCEPT SELECT 1d 960% (p_user_last) Site to 10 Michael (p_seer EXCEPT SELECT 1d 960% (p_user_last) Sagaw State (p_seer to 10 Michael (p_seer EXCEPT SELECT 1d 960% (p_user_last) Site (p_seer to 10 Michael (p_seer EXCEPT SELECT 1d 960% (p_user_last) Site (p_seer to 10 Michael (p_seer EXCEPT SELECT 1d 960% (p_user_last) Site (p_seer to 10 Michael (p_seer EXCEPT SELECT 1d 960% (p_user_last) Site (p_seer to 10 Michael (p_seer EXCEPT SELECT 1d 960% (p_user_last) Site (p_seer to 10 Michael (p_seer_last) Michael (p_seer EXCEPT SELECT 1d 960% (p_user_last) Michael (p_seer to 10 Michael (p_seer_last) Michael (p_seer_l		1 Document Emplo	3 FROM lp_user lu	
Incident Stapawa Task Attachment Command Instructure Attachment Command Instructure Instructure Stepsion St		🔥 Инциденты 🗸	<pre>4 WHERE lu.id IN (SELECT id FROM lp_user EXCEPT SELECT id FROM lp_user_last) 5) res</pre>	
Stagewing integration Attachment Command I therpoten I therpoten Step Step Step Step Step Step Group Step Construction I to Step in the Zerock I to Step Step Step Step Step Step Group Step Concerconsequence Information Template I LAPUSER OSmeptice Information Template I DAPUSER OSmeptice Message Template B gouese observes B gouese observes Structure Need Sending Sending Sending Type Mail Detail Sending Type Mail Detail Sending Type Mail Detail Sending Type Mail Detail Sending Type Sys Group ID Mailto Sys Group ID Mailto		E Incident >	6 WHERE cnt > 0	
Image: Step information Attachment Command Image: Step information Image: Step information Image: Structure information Image: Structure information		🖸 Задачи 🗸 🗸		
************************************		🔁 Task	Attachment Command	
Agent Construction of the structure of the s		🔀 Настройки 🗸	1 SELECT ''	
ave From Rpuser to ● Mrites Lo.1d 1N (SELECT id FRom Lpuser EXCEPT SELECT id FRom Lpuser_Lost) ● InfoZorok ● Pegaktrupobalue onewehra a Step ● InfoZorok ● Pegaktrupobalue onewehra a Step ● InfoZorok ● Pegaktrupobalue onewehra step ● Person ● InfoZorok ● Person ● Ressage Template ● Structure ● Romee ofivapyweno ((cnt)) noews ywernew same annucch nonesoestenns ● Asketa ● Romee ofivapyweno ((cnt)) noews ywernew samucch nonesoestens ● Asketa ● Romee ofivapyweno ((cnt)) noews ywernew samucch nonesoestens ● Asketa ● Romee ofivapyweno ((cnt)) noews ywernew samucch nonesoestens ● Asketa ● Romee ofivapyweno ((cnt)) noews ywernew samucch nonesoestens ● Asketa ● Romee ofivapyweno ((cnt)) noews ywernew samucch nonesoestens ● Asketa ● Romee ofivapyweno ((cnt)) noews ywernew samucch nonesoestens ● Asketa ● Romee ofivapyweno ((cnt)) noews ywernew samucch nonesoestens ● Asketa ● Romee ofivapyweno ((cnt)) noews ywernew samucch nonesoestens ● Asketa ● Rom		Agent	2 ,lu .displayname	
Group Settions PegaKTHpOBaHHe 3ЛeMeHTa B Step Indocent Indoc		Step	3 FROM lp_user lu 4 WHERE lu.id IN (SELECT id FROM lp_user_EXCEPT_SELECT id FROM lp_user_last)	
Settions Image: structure Image: structure <th></th> <th>Group</th> <th></th> <th></th>		Group		
Information Template		Settings		
Image: Structure Structure Structure Structure Anketa Anketa Anketa Structure <	5	InfoZorok	 Редактирование элемента в Step 	
Image: Section	Ŷ	Поиск коллекций	Information Template	
Image: Second secon		*8* Калры	LDAPUSER Обнаружена новая учетная запись пользователя	
■ Employee Message Template ● Structure ■ gomene o6Hapyweno {(cnt)} Hobbux yueTHbux sanucceй nonLsobare.nei/ ● Anketa ■ gomene o6Hapyweno {(cnt)} Hobbux yueTHbux sanucceй nonLsobare.nei/ ● Anketa ■ gomene o6Hapyweno {(cnt)} Hobbux yueTHbux sanucceй nonLsobare.nei/ ● Anketa ■ gomene o6Hapyweno {(cnt)} Hobbux yueTHbux sanucceй nonLsobare.nei/ ● Atruesi ■ ● Stock Need Sending ● Asset ■ ● Account Insert Attachment ● body ● ● Infosystem ■ ● Document ● ● Document ● ● Document Netil Detail ● Incident > ● Incident Sys Group ID Malito ● Task group_Idap_user_new		Person		
Structure В домене обнаружено ((cnt)) новых учетных записей пользователей Anketa В домене обнаружено ((cnt)) новых учетных записей пользователей Anketa Need Sending Stock Need Sending Stock Need Sending Asset Med Sending Asset Insert Attachment Uniforsystem body Infosystem Mail Detail Document Mail Detail Mail Detail Sys Group ID Malito Sys Group ID Malito group_Idap_user_new		Employee	Message Template	
Anketa Spravka Absence Cknag Stock Stock Asset Need Sending Need Sending Type Main Detail Vertuesersa Account Inforsystem Toporpandus Acsol through the sender Mail Detail Mail Detail Mail Detail Mail Detail Sys Group ID Mailto Sys Group ID Mailto Task		Structure	В домене обнаружено {{cnt}} новых учетных записей пользователей	
 Spravka Absence Cknag Stock AkTVBB Asset Vetrible sanucu Asset Vetrible sanucu Mułockicremai Mułockicremai Mułockicremai Mail Detail Mail Detail Mail Detail Sys Group ID Malito group_Jdap_user_new 		E Anketa		
Absence Cknag Stock Aktивы Asset Asset Account Account Insert Attachment body Insert Attachment body Mail Detail Vermal Document Document Document Document Document Document Document Sys Group ID Malito group_Jdap_user_new		Spravka		
Stock > ▲ Ктивы > ▲ Asset > ▲ Asset > ▲ VETHABE SAINKEN Insert Attachment ● Akcount > ● Account Insert Attachment ● Mikpocucremabi body ● Infosystem body ● Accounent body ● Document > ● Document html ● Incident > Sys Group ID Malito group_Jdap_user_new		CKDap		
Aktrusbu Need Sending Sending Type Asset Imail Yuetnuse sanucu Insert Attachment Yuetnuse sanucu body Account body Inforsystem body Inforsystem body KSC Software Mail Detail Document body Format Document Emplo html Muluquentia Sys Group ID Malito Sys Group ID Malito Imail		Stock		
Imail ✓ Imail <t< th=""><th></th><th>🗍 Активы 🗸</th><th>Need Sending Sending Type</th><th></th></t<>		🗍 Активы 🗸	Need Sending Sending Type	
Insert Attachment Insert Attachment Insert Attachment Inforpammal Inforpammal KSC Software Ackymental Document Document Emplo Incident Incident Sys Group ID Malito group_Jdap_user_new		🖨 Asset 🛛 🔶	✓ Включено mail	
Account Insert Attachment Image: Account body Inforpannel body Image: Account Body Format Image: Account body Image: Account body Image: Account body Image: Account Body Format Image: Account body Image: Account body Image: Account body Image: Account Body Format Image: Account body		🧧 Учетные записи 🗸		
Infosystem body Infosystem body Infosystem Mail Detail KSC Software Mail Detail Document Body Format Document html Incident Sys Group ID Malito Isak group_Idap_user_new		Account >	Insert Attachment	
Infosystem Infosytem		🚺 Инфосистемы 🗸	body v	
Image: KSC Software Mail Detail ~ Image: KSC Software Image: KSC Software Image: KSC Software Image: KSC Software Image: Document Image: KSC Software Image: KSC Software Image: KSC Software Image: KSC Software Image: Document Image: KSC Software Image: KSC Software Image: KSC Software Image: KSC Software Image: Document Emplo Image: KSC Software Image:		Infosystem		
Вody Format Вody Format Вody Format Вody Format html Muutugestras Sys Group ID Malito group_Jdap_user_new Л ×		КSC Software	Mail Detail	~
Body Format ♪ Document Emplo ♪ UHuµµµeнты ○ Incident > 3agaчи ♡ Task Body Format Body Format Intml Sys Group ID Malito Øroup_Jdap_user_new		🕞 Документы 🗸		
Image: Document Emplo html ✓ Image: Document Emplo html ✓ Image: Document Emplo Sys Group ID Mailto ✓ Image: Document Emplo group_Idap_user_new Image: Document Emplo		Document	Body Format	
▲ Инциденты ∨ ☺ Incident > ☑ Задачи ∨ ☑ Task group_Idap_user_new		🐧 Document Emplo	htmi	
Incident > Узадачи > Image: Sys Group ID Malito group_Jdap_user_new Image: Sys Group Jdap_user_new Image: Amage: Am		🛕 Инциденты 🗸 🗸		
☑ Задачи ✓ ☑ Task group_idap_user_new		incident >	Sys Group ID Malito	
		✓ Задачи ✓	group_Idap_user_new	
🔆 Насторйки 🗸		Тазк Настройки		

4.Активируем работу с помощью параметра active.

5. Проверяем в системном журнале, что работа запустилась и ошибок нет:



При добавлении новой учетной записи в LDAP в журнале и в почте появится соответствующий алерт:

Ę	контент Собы	тия 🛛			
	ID	When Created =	Information	Message	Sent
	ß	28 апреля 2025 г. 17:08	LDAPUSER Обнаружена нов	В домене обнаружено 1 новых учетных записей пользователей	×

3.4. Настройка автоматизации

В качестве примера автоматизации приведем пример автоматического создания учетной записи пользователя при появлении в штатном расписании нового работника.

1. Настраиваем Job:

- name: ldap_user_create
- active: выключено
- agent: выбираем агент, который будет выполнять работу

- sys step id: ссылка на step, который будет подключаться к LDAP и создавать учетные записи пользователей с данными из кадровой системы (создание описано ниже)

- trigger: interval (периодами)

- trigger params: { seconds: 60 }

< Редактирование элемента в Јор					
Name		Active			
ldap_user_create		Включено			
Sys Agent ID		Sys Step ID			
iz-agent01		= Idap_user_create			
		Создать Добавить существующий			
Trigger		Trigger Params			
interval		1 { 2 "seconds": 60			
		3 }			

2.Настраиваем Step автоматического создания учетных записей в LDAP:

- name: ldap_user_create

- sys job id: работа, в рамках какой работы будет выполняться step — ldap_user_create

- type: update
- language: python

- command: инструкция на языке python, которая получает данные о новом работнике из соответствующей коллекции, подключается к LDAP и создает учетную запись с необходимыми атрибутами (полный листинг инструкции алерта можно посмотреть в уже настроенной работе)

ldap_user_create		
Sys Job ID		
— Idap_user_create		
Создать Добавить	существующий	
Туре	Language	
	~ python	
update		
update Python Result Var		
update Python Result Var		

- 3.Активируем работу с помощью параметра «active» Job-а.
- 4. Проверяем в системном журнале, что работа запустилась и ошибок нет:

Е Соб	ытия 🛛			
	When Created =	Information	Message	Sent
	28 апреля 2025 г. 19:17	Daemon	Message: Start step "Idap_user_create"	

3.5.Регистрация пользователей и разграничение прав доступа

Регистрация пользователей системы осуществляется в модуле Пользователи. Здесь можно задать:

- имя пользователя
- адрес электронной почты
- первоначальный пароль
- необходимость ввода второго фактора
- параметры отображения интерфейса и др.

	InfoZorok	Попьзователя Добавление пользователя	
Ŷ	Все пользователи		
2	Administrator	Имя	Фамилия
	🛱 CR		Q
	💿 HR		
	oo IT	E-mail	Пароль
	© PS		6
	👰 Users		
		Аватар	
			Û
		Расположение	Должность
			Ċ
		Описание	
		Теги	
			\diamond

Разграничение прав доступа в системе выполняется с помощью создания политики прав доступа, где указываются какие права и к каким объектам системы будет иметь доступ получатель этой политики. Политику можно назначить на конкретного пользователя, или при унифицированном подходе - роли, а роль, в свою очередь пользователям. Роли можно включать друг в друга, создавая иерархию.

Пример определения политики:

С Политики доступа Политика IT					
Название политики *		lcon			
п		: چ	Supervised U	ser Circle	
Описание					
Permissions					
Коллекция	Действия				
an_account		Читать			
an_account_pn_person		Читать			
at_asset		Читать	Обновить		
at_asset_im_infosystem	Создать	Читать	Обновить	Удалить	
at_asset_pn_person		Читать			
de commuter					

Пример определения роли:

Роли пользователей		
С П Роль		
Название роли	Иконка роли	
ІТ	Supervised User Circle	
Описание		
Родительская роль		
выорать элемент		
Необязательная родительская роль, от которой эта роль наследует разрешения		
Policies		
= п		
Создать Добавить существующий		
	-	
ஃ Пользователи		
Пользователи в роли		
 Нет элементов 		
Создать Добавить существующий		

4. Устранение неисправностей

В случае выявления неисправности, причины некорректной работы можно отследить в системном журнале — коллекция Event.

Если устранить причины неисправности самостоятельно не представляется возможным, вы можете обратиться в службу технической поддержки вендора по адресу электронной почты <u>support@ib-nova.ru</u>. В обращении необходимо указать подробное описание и приложить содержимое системного журнала.