ГАРДА

Гарда Аналитика

Руководство администратора

garda.ai

2024

Тип документа: Руководство администратора

Дата выпуска: 30.05.2024

Версия: 1.24

Содержание

1. Введение

1.1. Аннотация

Данный документ представляет собой Руководство администратора к программному комплексу "Гарда Аналитика", предназначенному для выявления фактов угроз экономической безопасности организации.

1.2. Типографические соглашения

Обозначения и типографические соглашения, используемые в данном документе, приведены ниже.

Пример	Обозначение
Примечание: *текст*	Важная информация, требующая особого внимания
См. Руководство администратора	Ссылка на документ
Войти	Названия элементов веб-интерфейса и конфигурационных параметров.
http://www.example.com/	Гиперссылки

1.3. Использование имен, номеров телефонов, сетевых адресов

Приведенные в настоящем документе сведения о юридических и физических лицах, включая любые их данные, являются вымышленными, а IP-адреса и номера телефонов не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4. О компании

Гарда Технологии (входит в группу компаний Гарда) – разработчик семейства продуктов в области защиты данных и сетевой безопасности. Решения Гарда защищают данные крупнейших государственных организаций и корпораций, защищают 50% всего российского интернета от DDoS-атак, обеспечивают защиту цифровых сервисов и мероприятий федерального масштаба. Продуктовый портфель холдинга построен на основе технологий собственной разработки, которые не требуют сторонних лицензий, включены в Единый реестр российского ПО и сертифицированы ФСТЭК.

1.5. Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии":

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по московскому времени).
- Email: ga.support@gardatech.ru.

2. Обзор

2.1. Назначение Комплекса

Программный комплекс "Гарда Аналитика" (далее - ПК "Гарда Аналитика", Комплекс) - это система, реализующая выявление угроз экономической безопасности организации, поиск конфликта интересов, проведение внутренних расследований с использованием современных методов и инструментов работы с большими объёмами разнородных данных.

Основные задачи, решаемые Комплексом:

- Формирование досье физических и юридических лиц с использованием подключенных источников данных.
- Автоматизированное выявление негативных факторов в отношении физических и юридических лиц, в том числе кандидатов на приём, действующих сотрудников, потенциальных и действующих контрагентов.
- Выявление фактов связей между различными объектами, например, между действующими сотрудниками и контрагентами при проведении закупочных процедур.

2.2. Задачи администрирования Комплекса

В обязанности администратора ПК "Гарда Аналитика" входит:

- Подготовка сети предприятия к установке Комплекса.
- Установка Комплекса.
- Обновление Комплекса.
- Постинсталяционные настройки.
- Изменение настроек.
- Удаление Комплекса.
- Диагностика состояния Комплекса и исправление проблем.

3. Подготовка к установке

Перед установкой Комплекса следует выполнить следующие действия:

1. Подготовить сетевые настройки для ПК "Гарда Аналитика" (IP-адрес, шлюз, адрес DNS-сервера).
2. Подготовить доменную учетную запись для синхронизации с LDAP-сервером (Active Directory), если предполагается использование доменной аутентификации.
3. Подготовить список адресов контроллеров доменов, прокси-серверов, используемых в дальнейшем для работы источников.
4. Открыть необходимые порты для корректной работы Комплекса.

4. Установка и обновление модулей Комплекса

Установка и обновление модулей Комплекса описаны в соответствующих руководствах и производятся Службой технической поддержки.

Для получения рекомендаций обратитесь в Службу технической поддержки.

5. Постинсталляционные настройки

5.1. О настройках

После установки Комплекса необходимо выполнить:

- Настройку синхронизации Комплекса с LDAP-сервером (если предполагается использование).
- Проверку доступов и сетевых соединений/подключений к целевым источникам (БД, серверы с данными, интернет-ресурсы).

5.2. Установка сертификата SMTP-сервера

Для работы Email-оповещений по шифрованному каналу возможно потребуется установка сертификата SMTP-сервера (в зависимости от настроек SMTP-сервера, в большинстве случаев не требуется).

Для установки сертификата необходимо выполнить следующие действия:

1. Получить сертификат от SMTP-сервера с расширением .cer.
2. Скопировать полученный сертификат на сервер в папку **/ARCHIVE/**.
3. Зайти в папку **/ARCHIVE/** и выполнить команду:

```
[ip GardaAnalytics]# certmgr -add -c -v -m Trust *.cer
```

5.3. Настройка синхронизации с LDAP-сервером

Для использования доменной аутентификации настройте синхронизацию с LDAP-сервером.

Для настройки необходимо:

1. Перейти в **Настройки** → **Системные настройки** → **Настройки аутентификации через LDAP**.
2. Добавить домен.
3. Проверить соединение. Нажмите кнопку **Проверить соединение** и ожидайте сообщение о результате проверки.
4. Сохранить настройки синхронизации.

5.4. Критерии функционирования в штатном режиме эксплуатации

Корректное функционирование определяется корректной работой всех связанных служб и отсутствием ошибок в журналах работы компонентов.

5.5. Настройка интеграции с другими продуктами Гарда Технологии

Для получения рекомендаций обратитесь в Службу технической поддержки.

6. Настройки в веб-интерфейсе

6.1. Пользователи

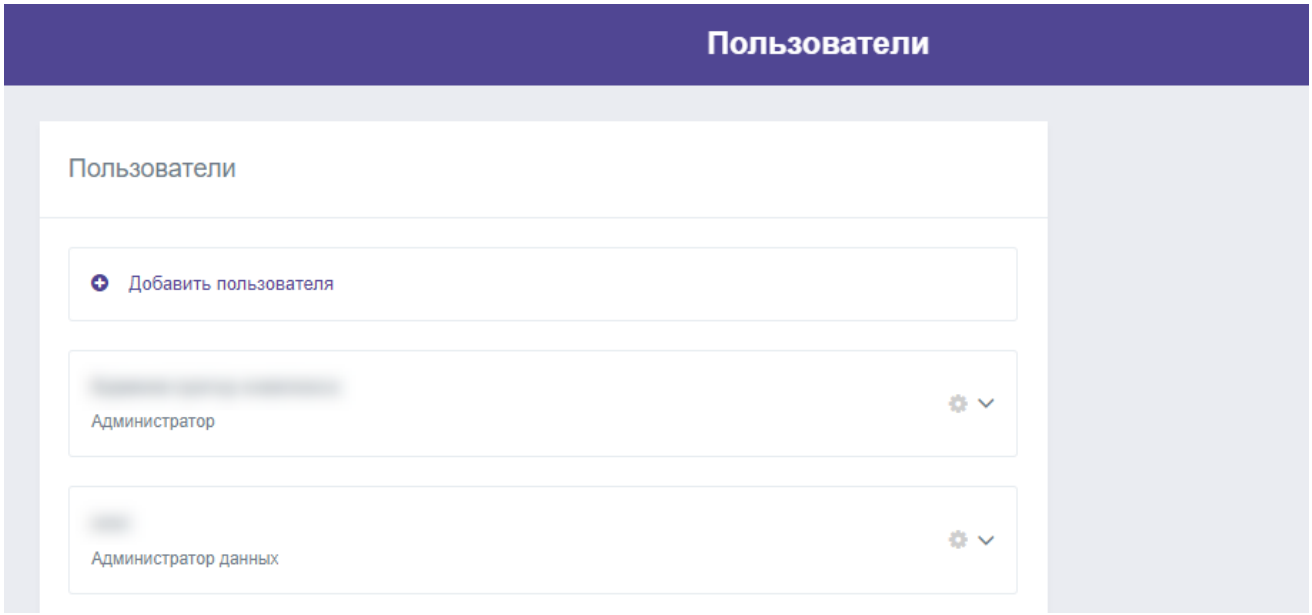
Этот раздел служит для управления доступом пользователей к функциям Комплекса.

В разделе представлено два блока:

- Пользователи.
- Роли.

Пользователи

Блок **Пользователи** содержит информацию о существующих пользователях Комплекса, а также позволяет добавлять новых пользователей, блокировать и удалять существующие учетные записи.



Добавление нового пользователя

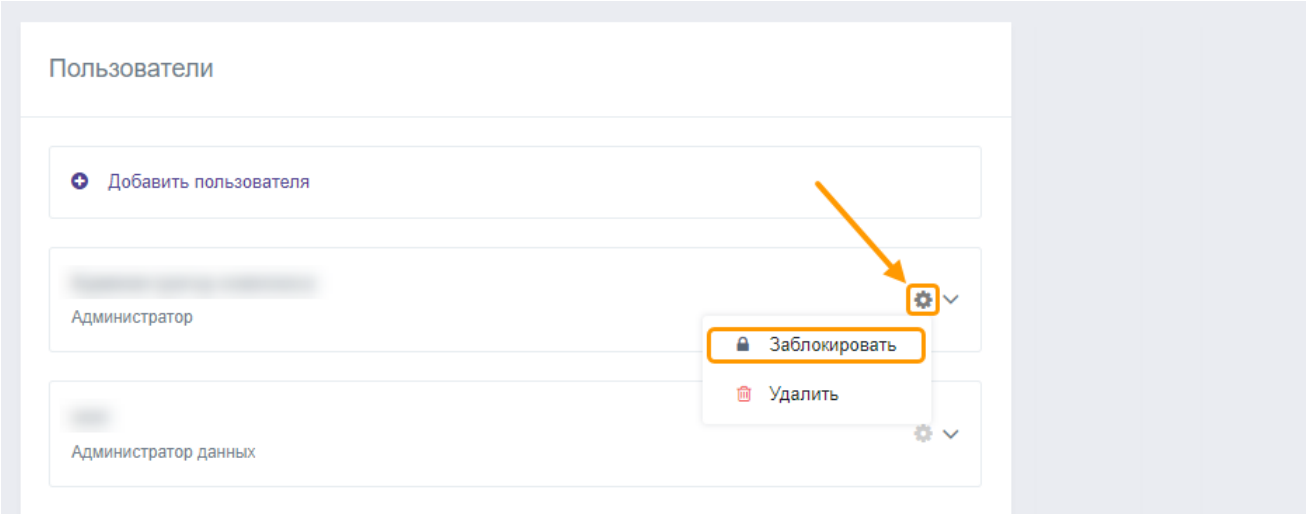
Чтобы добавить нового пользователя в Комплекс, выполните следующее:

1. Находясь на странице Пользователи, нажмите кнопку **Добавить пользователя**.
2. В открывшемся виджете задайте обязательные параметры.
3. Сохраните сделанные изменения.

Блокировка учётной записи пользователя

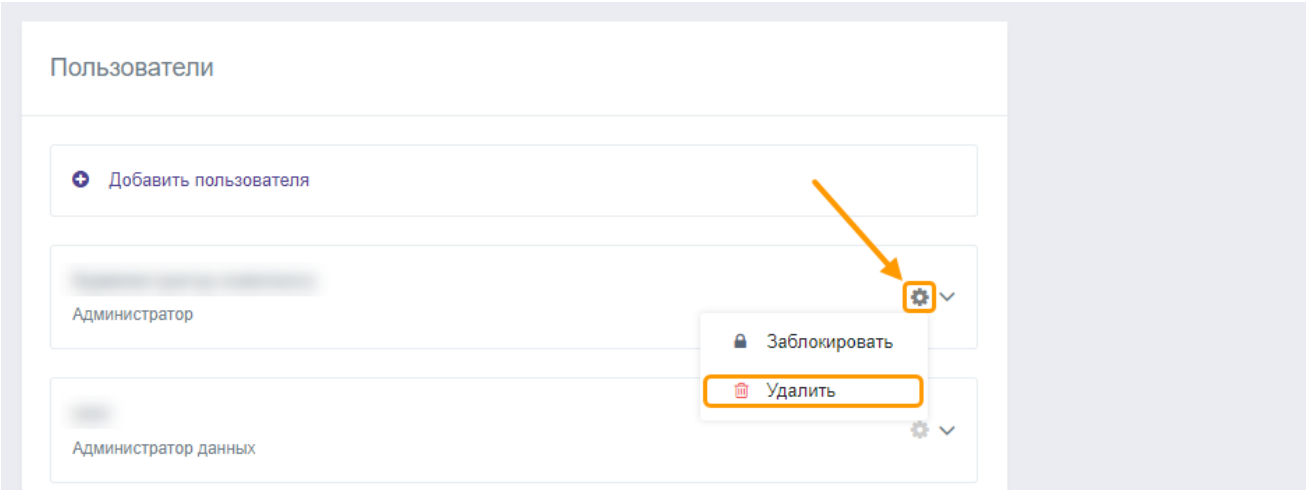
Если возникла необходимость ограничить доступ пользователя к Комплексу с последующей возможностью такой доступ предоставить, то для этого можно воспользоваться функцией блокировки пользователя.

Для этого в блоке **Пользователи** для соответствующей учётной записи необходимо активировать блокировку.



Удаление учётной записи пользователя

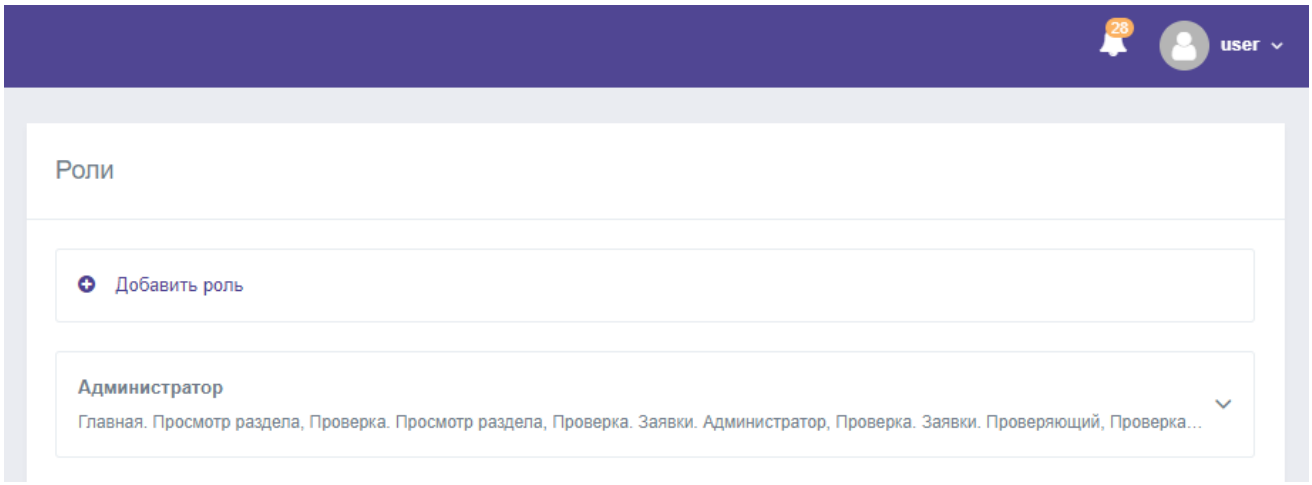
Для удаления соответствующей учетной записи в блоке **Пользователи** необходимо использовать функцию удаления.



Роли

Блок **Роли** служит для управления правами пользователей, позволяющими совершать те или иные действия в Комплексе.

Для определения прав пользователя необходимо создать роль. Каждая роль - эта группа прав. У каждого пользователя должна быть хотя бы одна роль.



Добавление новой роли

Чтобы добавить новую роль, выполните следующее:

1. Находясь на странице **Пользователи**, нажмите кнопку **Добавить роль**.
2. В открывшемся виджете задайте следующие обязательные параметры:
   - **Название роли** – уникальный идентификатор для группы прав.
   - **Доступ** – права доступа к функциям Комплекса и источникам данных (пометьте галочками нужные пункты в раскрывающемся иерархическом списке).
3. Сохраните сделанные изменения.

6.2. Системные настройки

6.2.1. Email-оповещения (Сервер SMTP)

Группа параметров, расположенная в блоке **Сервер SMTP**, предназначена для настройки взаимодействия Комплекса с почтовым сервером и задания адресов электронной почты, на которые будут высылаться оповещения об обнаруженных инцидентах в рамках правил.

6.2.2. Настройки аутентификации через LDAP

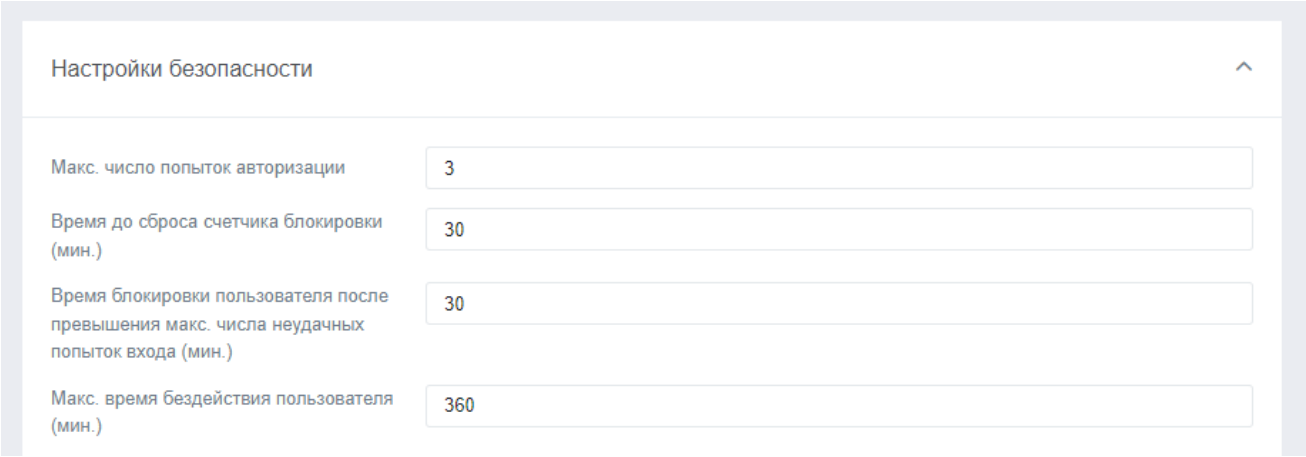
Чтобы у пользователя была возможность аутентификации через учётную запись (доменная авторизация), необходимо выполнить настройки аутентификации через LDAP.

6.2.3. Настройки безопасности

Этот блок позволяет задать следующие параметры:

- **Макс. число попыток авторизации** – число неудачных попыток, после которых доступ будет заблокирован на определённое время;

- **Время до сброса счетчика блокировки (мин.)** – время, за которое должно быть совершено указанное выше число неудачных попыток входа, чтобы сработала блокировка.
- **Время блокировки пользователя после превышения макс. числа неудачных попыток входа (мин.)** – время, на которое возможность входа для пользователя будет заблокирована;
- **Макс. время бездействия пользователя (мин.)** – время, через которое пользователь будет отключён от Комплекса.



6.2.4. Приоритет отображения информации из источников

В карточке Человека/Компании и в разделе **Поиск** на первое место выводится информация из того источника, которому задан высший приоритет.

Чтобы выставить приоритет источнику информации, перейдите в **Настройки** → **Системные настройки** → **Приоритет отображения информации из источников**.

Далее выберите тип объекта и укажите приоритет каждому источнику из списка путём ввода порядкового номера отображения или перетащив блок с источником выше или ниже по списку.

6.2.5. Шаблоны для экспорта в SIEM

Комплекс позволяет настраивать подключение к SIEM-системам и осуществлять экспорт журнала событий. Для интеграции с SIEM-системой необходимо создать шаблон с настройками подключения к системе:

1. Перейдите на страницу **Настройки** → **Системные настройки** → **Шаблон для экспорта в SIEM**.
2. Нажмите **Добавить шаблон**.
3. В открывшемся окне заполните поля.
4. Нажмите **Сохранить**.