



GARDA



Модуль Центр Управления

**Руководство
пользователя**

garda.ai

2024



Тип документа:	Руководство пользователя
Дата выпуска:	02.05.2024
Статус документа:	Released
Версия:	5.2

ООО "Гарда Технологии"
Все права сохраняются за правообладателем.

ООО "Гарда Технологии" оставляет за собой право вносить изменения в содержащуюся в данном документе информацию без предварительного уведомления.

ИНФОРМАЦИЯ О ПРАВЕ СОБСТВЕННОСТИ

Информация, содержащаяся в данном документе, является собственностью ООО "Гарда Технологии". Никакая часть этого документа не может быть воспроизведена или заимствована в какой бы то ни было форме или каким-либо способом – в графическом, электронном виде или механическим путем, включая фотокопирование, запись, в том числе и на магнитные носители, или любые другие устройства, предназначенные для хранения информации – без письменного разрешения ООО "Гарда Технологии". Подобное разрешение не может быть выдано третьей стороной, будь то организация или частное лицо.



Содержание

1 Введение	4
1.1 Аннотация.....	4
1.2 Типографические соглашения.....	4
1.3 Использование имен, номеров телефонов, сетевых адресов.....	4
1.4 О компании.....	4
1.5 Техническая поддержка.....	5
2 Назначение Модуля	6
3 Работа с Модулем	7
3.1 ПО для работы пользователя.....	7
3.2 Вход в Комплекс.....	7
3.3 Парольная политика.....	8
3.4 Общий вид Модуля.....	10

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство пользователя к программному модулю "Центр Управления" (далее – Модуль), входящему в состав программного обеспечения "Гарда БД" (далее – Комплекс).

1.2 Типографические соглашения

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

Пример	Обозначение
Примечание: <i>текст</i>	Важная информация, требующая особого внимания
<i>См. Руководство администратора</i>	Ссылка на документ
Войти	Названия вкладок, кнопок и конфигурационных параметров в веб-интерфейсе
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: gbd.support@gardatech.ru.

2 Назначение Модуля

Модуль предназначен для многопользовательского доступа к интерфейсу Комплекса: аудита и мониторинга обращений к базам данных, внесения изменений в конфигурацию Комплекса, запуска фоновых задач.

3 Работа с Модулем

3.1 ПО для работы пользователя

Доступ к Модулю осуществляется с использованием одного из следующих веб-браузеров:

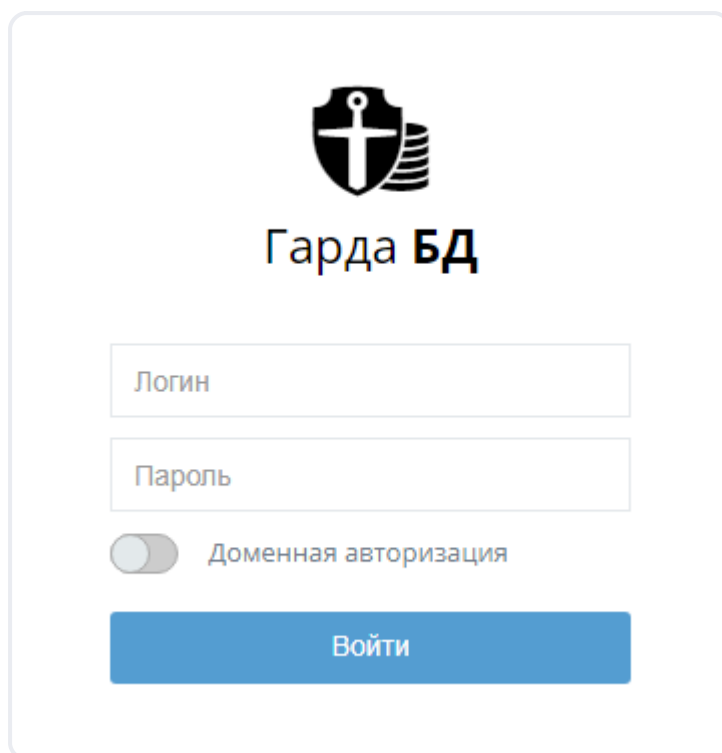
- Google Chrome версии 122.0.6261.112 и выше;
- Mozilla Firefox версии 123.0.1 и выше.

3.2 Вход в Комплекс

Для доступа к веб-интерфейсу Комплекса:

1. [Откройте веб-браузер.](#)
2. В адресной строке веб-браузера введите `http://IP-address`, где IP-address – это IP-адрес, указанный администратором.
3. В открывшемся окне укажите имя пользователя и пароль в соответствующих полях и нажмите **Войти**.
 - 3.1. Для входа в Комплекс при помощи доменной учетной записи активируйте переключатель **Доменная авторизация**, укажите имя пользователя и пароль доменной учетной записи и нажмите **Войти**.

Примечание: Функция доменной авторизации доступна только при настроенном сервере LDAP.



4. При первом входе в Комплекс ознакомьтесь с лицензионным соглашением, прочитав его до конца. Если вы согласны с условиями соглашения, нажмите **Принять**.



После входа в Комплекс на экране появится главная страница веб-интерфейса.

3.3 Парольная политика

Для соответствия лучшим требованиям в области информационной безопасности в Комплексе задан список настроек парольной политики.

Для настройки парольной политики в соответствии с внутренними требованиями безопасности компании нажмите на имя пользователя в правом верхнем углу интерфейса и выберите **Парольная политика**.

Примечание: Раздел доступен только пользователям с ролью **Главный администратор**.

В Комплексе доступны следующие настройки безопасности входа:

- Базовые настройки:
 - срок действия пароля;
 - минимальное количество символов в пароле;
 - срок действия активной сессии;
 - срок действия первичного пароля.
- Использование символов в пароле:
 - наличие в пароле прописных и строчных букв алфавита;
 - наличие в пароле спецсимволов (@, #, \$, &, *, % и т.п.);
 - наличие в пароле цифр и минимальное их количество.
- Изменение пароля:
 - количество предыдущих паролей, с которыми не должен совпадать новый пароль;
 - требование смены пароля при первом входе.
- Блокировка:
 - количество неуспешных попыток входа до блокировки пользователя;
 - срок действия блокировки;

Примечание: В результате блокировки учетной записи авторизация в Комплексе не доступна до разблокировки учетной записи. Разблокировка выполняется [автоматически по истечении периода блокировки](#), [автоматически после успешной доменной авторизации](#) или вручную.

- **Автоматическая разблокировка** – деактивируйте данный переключатель, если автоматическая разблокировка запрещена. По умолчанию данная функция включена.

- **Автоматическая разблокировка доменных пользователей после успешной авторизации** – активируйте данный переключатель, если хотите позволить доменным пользователям авторизовываться в Комплексе даже в той ситуации, когда они заблокированы. Данная функция полезна тем, что позволяет контролировать доступ к Комплексу только на уровне домена, отсекая контроль доступа на уровне Комплекса. По умолчанию данная функция выключена.

Примечание: При включенной функции **Автоматическая разблокировка доменных пользователей после успешной авторизации** Комплекс становится уязвимым для брутфорс атаки.

- **Разлогинить всех** – незамедлительная остановка всех активных сессий;
- **Сменить пароль для всех** – принудительное завершение срока действия пароля для всех пользователей.

The screenshot shows the 'Парольная политика' (Password Policy) settings page. The page has a red header with the title 'Парольная политика' and a user profile 'admin'. Below the header, there are two buttons: 'Разлогинить всех' (Log out all) and 'Сменить пароль для всех' (Change password for all). The main content area is titled 'Настройки безопасности' (Security Settings) and contains several sections:

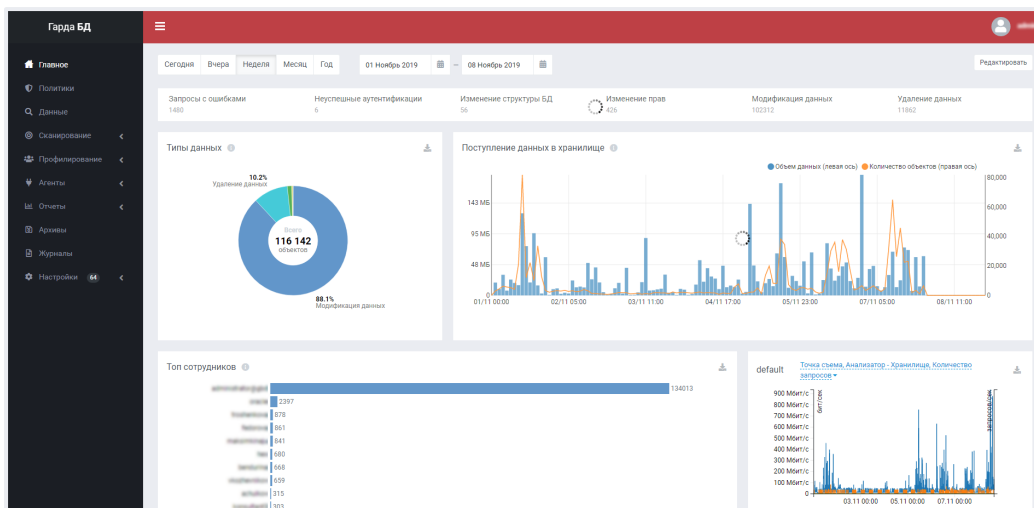
- Срок действия пароля ***: 90 дней
- Минимальная длина пароля ***: 7 символов
- Выход при бездействии в течение ***: 15 минут
- Срок действия первичного пароля**: 14 дней
- Использование символов в пароле**:
 - Буквы разного регистра (пример: PassWord)
 - Спецсимволы (пример: p@ssw0rd_)
 - Цифры (пример: password12345)
 - Минимальное количество цифр**: 2
- Изменение пароля**:
 - Пароль не должен совпадать с**: 4 предыдущими
 - Требовать смену пароля при первом входе в систему
- Блокировка***:
 - Блокировать пользователя после**: 3 неверных попыток ввода
 - Автоматическая разблокировка
 - Период блокировки**: 30 минут
 - Автоматическая разблокировка доменных пользователей после успешной авторизации (with a red warning icon)

At the bottom of the settings area, there is a blue button labeled 'Применить' (Apply).

После изменения настроек безопасности нажмите **Применить**.

3.4 Общий вид Модуля

Ниже изображена страница Модуля.



В левой части страницы расположена панель меню, которая содержит список страниц, доступных пользователю Комплекса:

- **Главное** – отображает статистическую информацию о работе Комплекса.
- **Политики** – содержит политику тотального перехвата и политики информационной безопасности.
- **Данные** – содержит инструменты фильтрации и анализа собранных данных: операций в БД и веб-приложениях.
- **Сканирование** – содержит настройки и результаты сканирования БД на типы данных, уязвимости и привилегии пользователей.
- **Профилирование** – содержит настройки функции поведенческого анализа действий пользователей и возможности Комплекса по выявлению отклонений от профилей пользователей.
- **Агенты** – содержит настройки агентов контроля подключений к БД, списки правил и журналы блокировок трафика.
- **Отчеты** – содержит аналитические отчеты и графики по операциям с БД.
- **Архивы** – предоставляет возможности для работы с архивами собранных данных.
- **Журналы** – содержит системные журналы.
- **Настройки** – содержит настройки учетных записей пользователей Комплекса, синхронизации с сервером LDAP, управления анализаторами, постановки баз данных на контроль, настройки списков критериев и интеграции с SIEM-системами, настройки Email-

оповещений и профилей баз данных, резервное копирование настроек Комплекса, список фоновых задач и диагностику комплекса.

В правой части страницы расположена область отображения данных в соответствии с выбранным пунктом меню.

По нажатию на имя пользователя в правом верхнем углу интерфейса раскрывается список, который содержит следующие элементы:

- **Парольная политика** – переход в раздел [Парольная политика](#);
- **Лицензия** – переход в раздел Лицензия.
- **Справка** – открывает Руководство пользователя и Руководство администратора;
- **О программе** – содержит информацию о версии программы и контроле целостности Комплекса;
- **Выход** – кнопка выхода из Комплекса.

