



ГАРДА



Гарда Аналитика

Описание ПО

garda.ai

2024



Тип документа: Описание ПО
Дата выпуска: 30.05.2024
Статус документа: Released
Версия:

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 Общая информация	6
3 Архитектура	7
3.1 Установка.....	7
3.2 Типовая схема внедрения.....	7
3.3 Аппаратное обеспечение.....	8
4 Функциональные возможности	9
4.1 Функциональные модули.....	9
4.2 Список источников для получения информации.....	9
4.3 Поиск информации.....	11
4.4 Построения графа связей.....	12
5 Примеры решаемых задач	13

1 Введение

1.1 Аннотация

Данный документ представляет собой описание программного комплекса "Гарда Аналитика", предназначенного 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 Общая информация

Комплекс предназначен для автоматизации бизнес-процессов, направленных на проведение комплексных проверок кандидатов и сотрудников заказчика, потенциальных и действующих контрагентов Компании, поиска связей между различными сущностями, в том числе для выявления конфликтов интересов между различными категориями кандидатов, сотрудников и контрагентов.

Комплекс поддерживает следующие функции:

- Интеграция с внешними и внутренними информационными системами заказчика.
- Сбор данных об объектах проверок из нескольких источников данных с последующим анализом и централизованным хранением.
- Формирование досье проверяемых объектов и справок по результатам проверок.
- Гибкая настройка факторов для проведения проверок.
- Визуализация выявленных связей между различными объектами.
- Автоматизация полного цикла проверок кандидатов и контрагентов – получение и отправка данных во внутренние системы заказчика.
- Автоматизация мониторинга действующих сотрудников и контрагентов для оперативного выявления факторов риска.
- Формирование единой базы проверок.

Комплекс интегрируется с внешними и внутренними источниками заказчика, что позволяет оценить все связанные с заказчиком объекты, их факторы риска и связи. Загрузка данных из внешних источников в БД Комплекса и встроенная база факторов позволяют использовать Комплекс сразу после установки, а настройка ролевой модели позволит разграничить доступ к данным для пользователей разных филиалов и дочерних компаний.

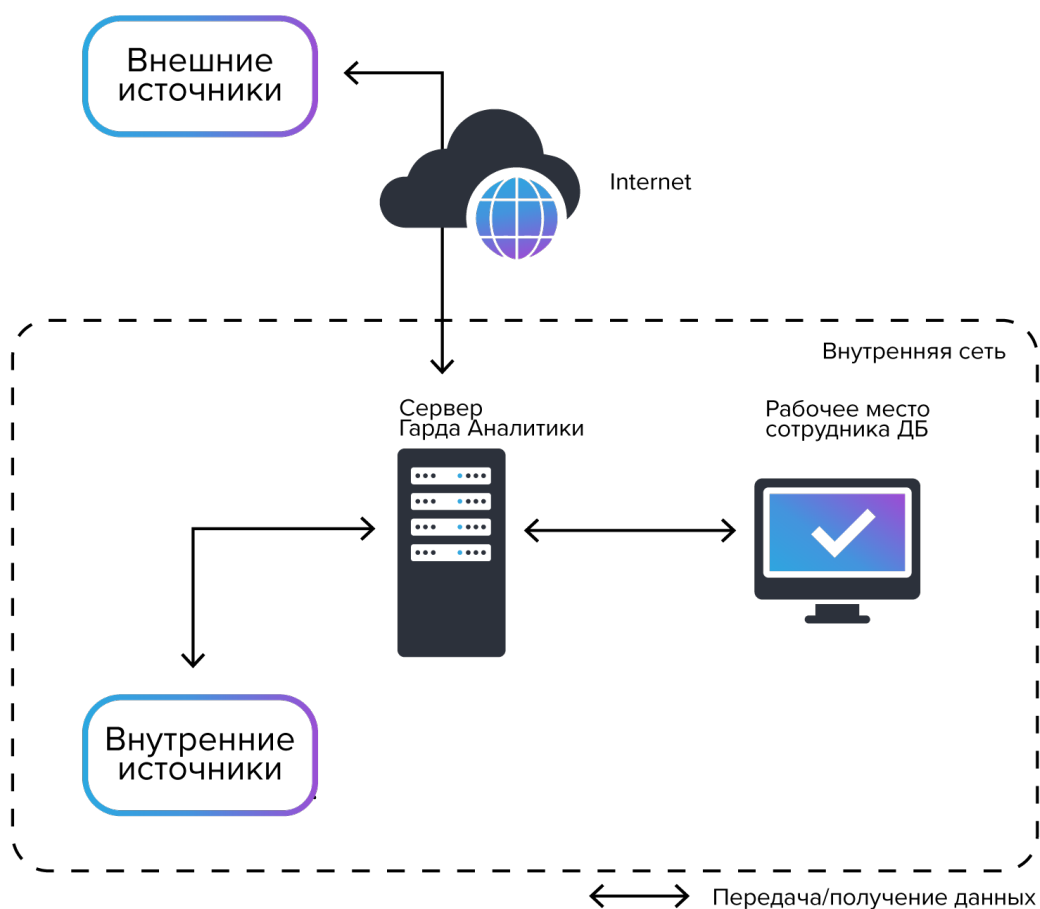
3 Архитектура

3.1 Установка

Комплекс устанавливается внутри периметра заказчика. Требуется выход в интернет для обновления и получения данных.

3.2 Типовая схема внедрения

Типовая схема внедрения представлена на рисунке ниже.



3.3 Аппаратное обеспечение

Требования к аппаратной/виртуальной части Комплекса представлены в таблице ниже.

	Минимальные требования	Рекомендуемые требования
CPU	16 ядер, без включенного гипертрединга	20 ядер, без включенного гипертрединга
ОЗУ	128 Гб	256 Гб
HDD (хранение)	5 Тб	5 Тб
HDD (система)	1 Тб	1 Тб
Карта сетевая	2-х или 4-х портовая	2-х или 4-х портовая
Количество IP адресов	2 (IP адрес IPMI + IP адрес management)	2 (IP адрес IPMI + IP адрес management)

4 Функциональные возможности

4.1 Функциональные модули

Комплекс состоит из следующих функциональных модулей:

- Модуль хранения и представления данных. Служит для хранения информации, связанной с различными сущностями – физические и юридические лица, адреса, телефоны и др. Срок хранения данных ограничивается объемом дискового пространства, выделяемого под хранилище.
- Модуль проверки. Необходим для настройки факторов, шаблонов проверки, работы с заявками и объектами, поставленными на контроль.
- Модуль связей. Необходим для графического представления связей, имеющихся в Комплексе, а также для поиска связей между различными объектами, группами объектов и объектами внутри групп.
- Модуль администрирования. Обеспечивает разграничение доступа к Комплексу на основе ролевой модели, возможность создания ролей и назначения бизнес-действий по каждой роли, а также настройки Комплекса, в том числе интеграцию с Active Directory, почтовым сервером, экспорт в SIEM и пр.
- Модуль интеграции с внешними источниками. Набор коннекторов к внешним источникам.
- Модуль интеграции с внутренними источниками. Набор коннекторов к внутренним источникам.
- Модуль отчетности. Позволяет формировать отчеты по накопленным в Комплексе данным.
- Модуль журналирования. Обеспечивает логирование действий пользователей в Комплексе.

4.2 Список источников для получения информации

Комплекс получает, обрабатывает и сохраняет данные от систем-источников, указанных ниже. Помимо описанных ниже базовых источников данных

имеется возможность добавления в Комплекс дополнительных источников и справочников информации.

Базовые внешние источники:

- ЕГРЮЛ.
- ЕГРИП.
- Бухгалтерская (финансовая) отчётность.
- БД Исполнительных делопроизводств ЮЛ (БД ФССП).
- Арбитражные дела.
- OpenStreetMap.
- Яндекс Геокодер.
- Дисквалифицированные лица.
- Данные о доходах и расходах ЮЛ.
- Среднесписочная численность.
- Сведения об уплаченных налогах и сборах.
- Сведения о штрафах, недоимках и пени.
- ЮЛ, в состав исполнительных органов которых входят дисквалифицированные лица.
- Адреса, указанные при государственной регистрации в качестве места нахождения несколькими юридическими лицами.
- Государственный реестр аккредитованных филиалов, представительств иностранных юридических лиц.
- Реестр недействительных паспортов МВД.
- Перечень действующих террористов и экстремистов, предоставляемый Росфинмониторингом.
- Реестр проверок Генеральной прокуратуры.
- Реестр гос. контрактов по 44 ФЗ, 94-ФЗ, 223-ФЗ, ПП-615.
- Реестр недобросовестных поставщиков по 44-ФЗ, 94-ФЗ, 223-ФЗ, ПП-615.
- Проверка на самозанятость.
- Стандартизация адресов.
- Сервис подсказок при вводе адреса.
- Реестр иноагентов ФЛ/ЮЛ, утверждённый Министерством юстиций РФ.

- Консолидированные группы налогоплательщиков.
- Реестр ЮЛ с выявленными признаками нелегальной деятельности на финансовом рынке.

Базовые внутренние источники:

- Установленная у заказчика система управления персоналом (по имеющемуся шаблону обмена данными).
- Установленная у заказчика система управления и взаимодействия с контрагентами и договорами (по имеющемуся шаблону обмена данными).
- Дополнительные источники:
 - Контроль кадров МФ.
 - СПАРК-Шлюз.
 - Источники для получения дополнительной информации о ФЛ.

4.3 Поиск информации

Пользователю доступны следующие режимы поиска:

- **Простой поиск** – позволяет производить поиск объектов:
 - Для физических лиц по любому из следующих параметров: ИНН, ФИО, Фамилия, Имя, Отчество, Дата рождения, Паспорт, Персональный номер, ОГРНИП, Учетная запись;
 - Для юридических лиц по любому из следующих параметров: ИНН, ОГРН, КПП, название.
 - Другие сущности по доступным атрибутам.
- **Расширенный поиск** – позволяет производить поиск объектов на основании сразу нескольких поисковых параметров и связей с другими объектами.

Возможна постановка сохраненного поискового запроса на контроль по факторам проверки. Если объект, подпадающий под поисковый запрос, также попадает под фактор проверки, пользователю будет приходить уведомление. Аналогичное уведомление будет приходить, если объект перестал попадать под фактор проверки.

4.4 Построения графа связей

Комплекс предоставляет возможность обнаружения нелегитимных/подозрительных отношений (связей) между субъектами контроля. Данная возможность предусматривает построение графа связей на основе задаваемых пользователем параметров. В качестве субъектов контроля могут выступать люди, компании, адреса, телефоны, факсы, почта, мессенджер, ВУЗ, социальные сети, подразделения, документы, арбитражные дела, транспорт. На графе субъекты контроля представлены как вершины, изображенные в форме круга, а связи - в виде соединяющих ребер. Помимо явных связей, с помощью графа можно выявить неявные связи, т.е. связи между субъектами, например, через общий контакт. Также Комплекс позволяет находить связи между группами различных объектов или объектами, попадающими под сохранённый поисковый запрос.

Функции при работе с графом связей

Для работы с графом доступны следующие функции:

- Фильтрация связей по типу вершин и типу связей;
- Фильтрация связей по времени;
- Просмотр информации по вершине;
- Автоматическое построение графа связей между:
 - Двумя вершинами.
 - Несколькими вершинами.
 - Вершинами и группами объектов.
 - Группами объектов.
 - Вершинами и сохранёнными фильтрами.
 - Сохранёнными фильтрами.
 - Группами объектов и сохранёнными фильтрами.

Работа с журналами

Все действия пользователей журналируются. Данные представляются либо в табличном виде, либо в виде графиков. Журнал защищён от удаления. Возможен экспорт журнала в формате .xlsx, .csv, а также в SIEM-систему.

5 Примеры решаемых задач

- Выявление конфликта интересов сотрудников компании при проведении закупок;
- Выявление рисков при приеме кандидатов на работу;
- Выявление конфликта интересов при приёме кандидатов на работу;
- Проверка контрагентов на благонадежность;
- Обнаружение фактов подозрительных связей между сотрудниками компании, сотрудниками и представителями компаний-контрагентов, сотрудниками и клиентами;
- Проведение внутренних расследований;
- Формирование досье сотрудника компании;
- Формирование единой базы проводимых проверок.