

## Тестовое задание №1

---

Информационная эра положила начало передовому развитию информационных технологий, что послужило сильным толчком для изменений в способах обработки, хранения и передачи информации. Компании начали использовать большие данные и различные аналитические инструменты для оптимизации своих процессов.

Однако с ростом возможностей, приходят и новые угрозы. Увеличение объема данных создало благоприятную среду для кибератак и угроз безопасности. Атаки становятся всё более сложными, а их последствия могут быть очень серьезными. Чтобы справиться с этими проблемами и снизить цифровые риски, важно правильно защищать информацию.



Digital Risk Protection - это AI-платформа, обеспечивающая безопасность компании в цифровой среде. С её помощью можно мониторить активность киберпреступников и своевременно пресекать нарушения.

### Направления цифровых угроз:

- Фишинг
- Мошенничество
- Неправомерное использование товарного знака
- Контрафакт
- Пиратство
- Несоблюдение партнерской политики
- Утечки данных
- Неправомерное использование личности

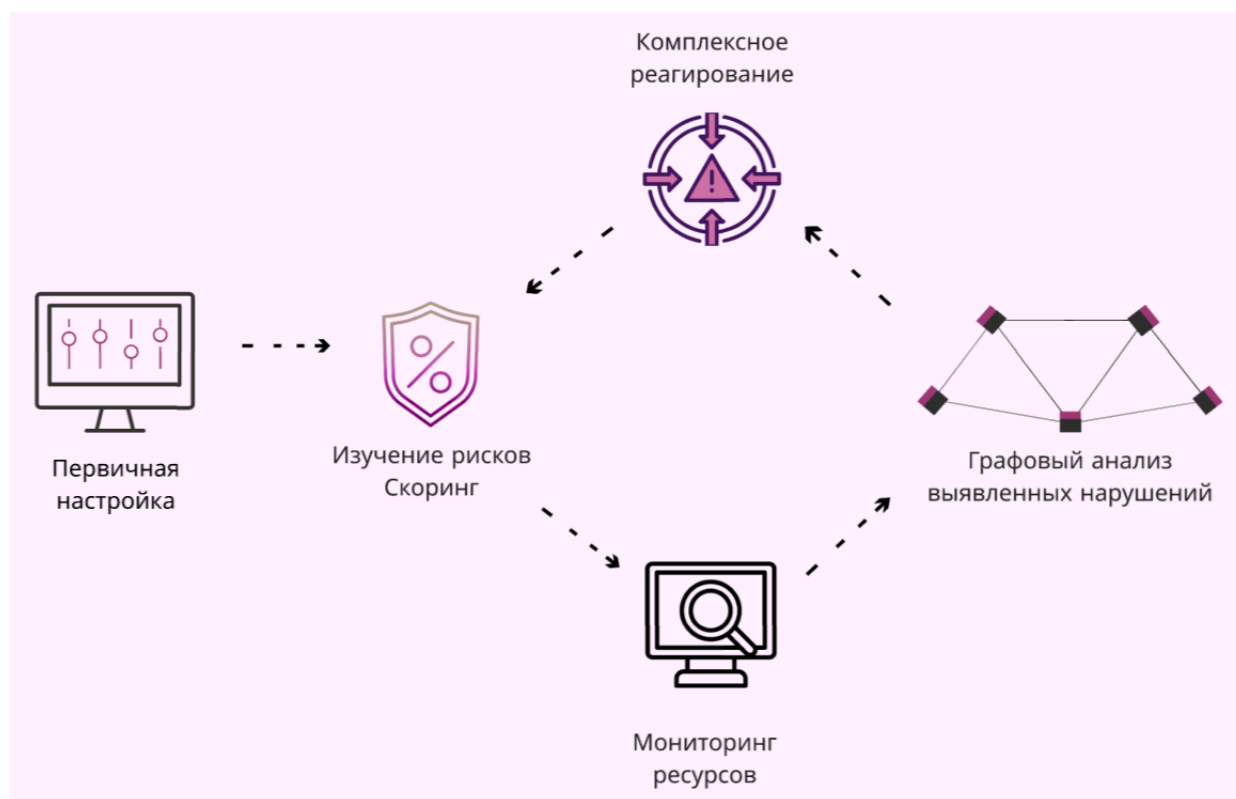
Столкновение с подобными угрозами может привести к серьезным последствиям, включая сбои в внутренних процессах. Решение инцидентов с утечками данных или кибератаками занимают время и усилия. Поэтому компании должны заранее принимать меры для защиты своих цифровых активов и минимизации рисков.

---

Digital Risk Protection предлагает комплексные решения для борьбы с угрозами. Платформа проводит мониторинг, выявляет и быстро устраняет потенциально мошеннические ресурсы.

Для этого используется методология F.A.C.C.T, которая анализирует связи между ресурсами. На основе собранных данных формируется скоринг, который помогает понять уровень риска для бизнеса. Он включает в себя анализ уязвимостей, оценку потенциальных угроз и определение вероятности их возникновения.

Информация представлена в виде графа с визуализацией общих признаков обманных схем: параметров доменов, цепочек перенаправлений, файлов различных форматов и указанных адресов. Искусственный интеллект анализирует эти данные и своевременно реагирует на угрозы.



Когда обнаруживается угроза, платформа начинает комплексное реагирование. В него входят автоматические меры по устранению угрозы, уведомление источников потенциальных рисков и блокировка ресурсов. На завершающем этапе платформа создает отчет о выявленных рисках и предпринятых действиях. Отчет помогает компаниям лучше понять свои уязвимости и разработать стратегии для улучшения безопасности в будущем.

---

Работа с платформой поделена на несколько модулей:

### Антимошенничество

Работа модуля направлена на выявление ресурсов, связанных с нелегитимным использованием цифровых материалов компании и её бренда в мошеннических или рекламных целях. Платформа сканирует подозрительные домены, фейковые аккаунты в социальных сетях и фишинговые страницы, представляющие ловушку для посетителей и несущие репутационные риски компании.

## Антиконтрафакт

Представляет собой набор инструментов для борьбы с контрафактной продукцией, распространяющейся по сети. Для этого модуль отслеживает интернет-пространство и, используя технологии сканирования, отбирает подозрительные источники. После формируется отчёт о выявленных случаях контрафакта, который можно использовать для дальнейших юридических действий против нарушителей. Также модуль имеет возможность отправки писем в предприятия, осуществляющие продажу контрафактной продукции.

## Антипиратство

Для борьбы с пиратством и нарушениями интеллектуальной собственности используется антипиратский модуль. Его функционал включает в себя выявление и предотвращение распространения защищенных авторским правом материалов. Подобный подход способствует уменьшению случаев незаконного использования цифровых активов компании и снижению рисков понести репутационные убытки.

## Выявление утечек данных

Человеческого мониторинга недостаточно для проведения качественных и многочисленных проверок утечек информации. Данный модуль обнаруживает источники нарушения конфиденциальности, опубликованные в сети.

## Защита VIP-персон

Модуль проверяет всю доступную персональную информацию о личности в интернете: фейковые аккаунты, дезинформирующие материалы и утечки. Затем сортирует данные по степени угрозы.

---

В заключение, Digital Risk Protection (DRP) представляет собой мощный инструмент, который помогает компаниям эффективно справляться с растущими угрозами в цифровом пространстве. Его ценности и достоинства заключаются в проактивной защите, мониторинге в реальном времени, аналитике и прогнозировании, что позволяет организациям не только реагировать на инциденты, но и предотвращать их.

С помощью DRP компании могут значительно снизить финансовые потери, улучшить свою репутацию и обеспечить комплексный подход к безопасности. Легкость интеграции с существующими системами и предоставление обучения для сотрудников делают эту платформу доступной и удобной для использования.

В условиях современного мира, где киберугрозы становятся все более сложными и разнообразными, применение Digital Risk Protection становится не просто желательным, а необходимым для обеспечения устойчивости и безопасности.

бизнеса. Инвестируя в DRP, организации не только защищают свои цифровые активы, но и создают основу для уверенного и безопасного будущего в цифровой экономике.

## Тестовое задание №2

### Глоссарий

Брандмауэр	Система безопасности, которая контролирует входящий и исходящий сетевой трафик. Защищает сеть от несанкционированного доступа и атак.
Домен	Уникальное символьное имя, соответствующее IP-адресу ресурса в Интернете. ( Пример: www.facct.ru)
Прокси-сервер	Промежуточный сервер, осуществляющий обмен информацией между пользователем и интернет-ресурсом. Обеспечивает безопасность передачи данных и контролирует сетевой трафик.
Сигнатурный анализ	Метод обнаружения угроз, основанный на выявлении характерных признаков мошеннических схем в Интернете путем сравнения ресурсов с выявленными признаками.
Фишинг	Метод мошенничества, основанный на получении доступа к ценным цифровым активам и конфиденциальной информации пользователя.
DNS-сервер	Сервер, который преобразует доменные имена в IP-адреса, позволяя пользователям легко находить веб-сайты.
IDS (Intrusion Detection System)	Система обнаружения вторжений, которая мониторит сетевой трафик и системы на предмет подозрительной активности и потенциальных угроз.
IP-адрес	Уникальный числовой идентификатор, присвоенный каждому устройству в сети. Позволяет пользователю отправлять и получать данные.
SSL (Secure Sockets Layer)	Протокол, обеспечивающий шифрование данных между пользователем и сервером, что гарантирует безопасность передачи информации.
SSH (Secure Shell)	Сетевой протокол, обеспечивающий безопасное удаленное взаимодействие между сервером и клиентом. Позволяет управлять и обмениваться данными.

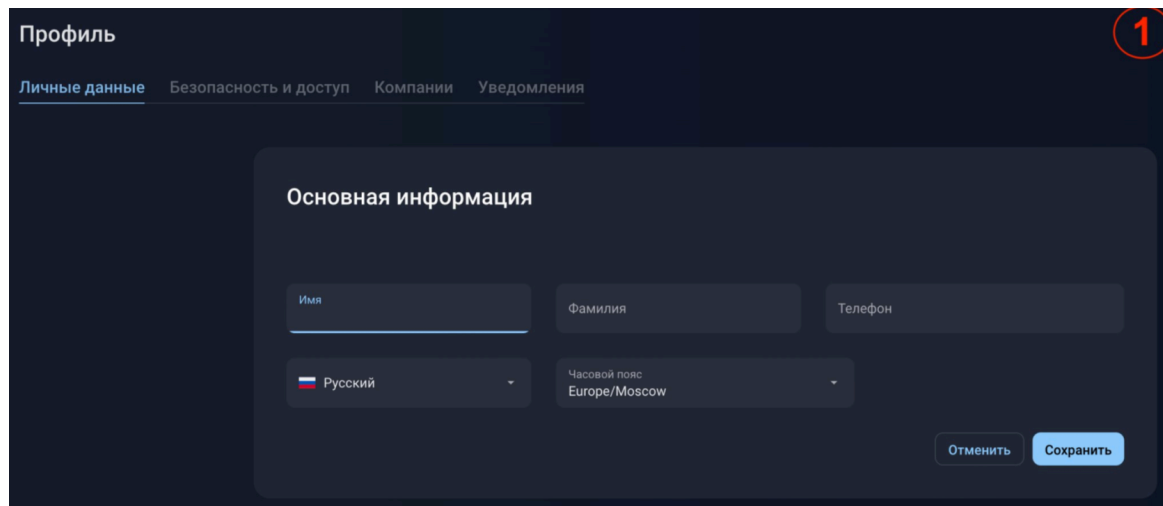
## Тестовое задание №3

Инструкция по первичной настройке пользователя:

1. Для настройки учетной записи сначала войдите в профиль.

### Личные данные

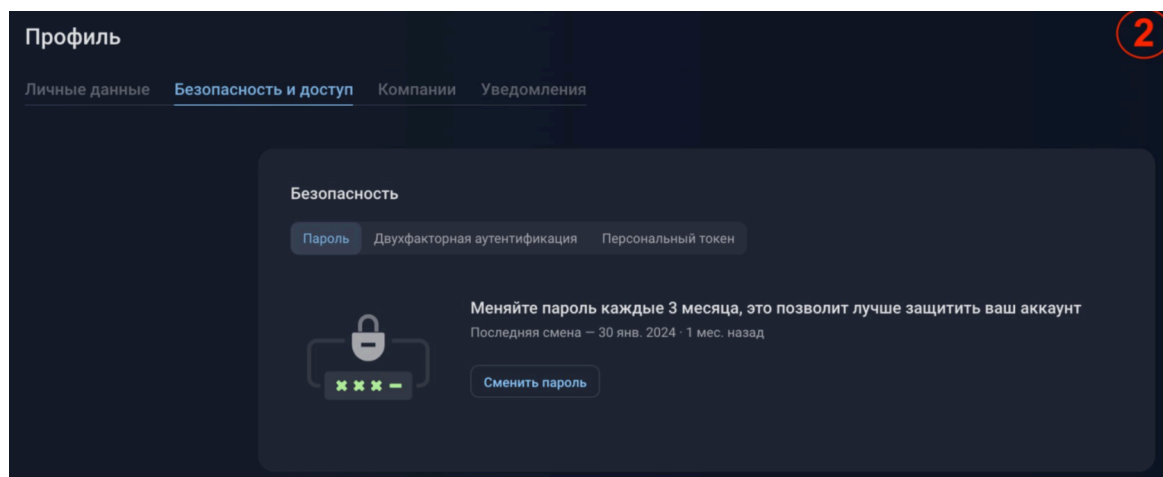
- Заполните основную информацию пользователя, указав в форме имя, фамилию и контактные данные. В выпадающем меню выберите нужный язык и часовой пояс.
- Убедившись в корректности введенной информации, нажмите кнопку сохранения.



2. Для защиты аккаунта, поменяйте предустановленный пароль пользователя.

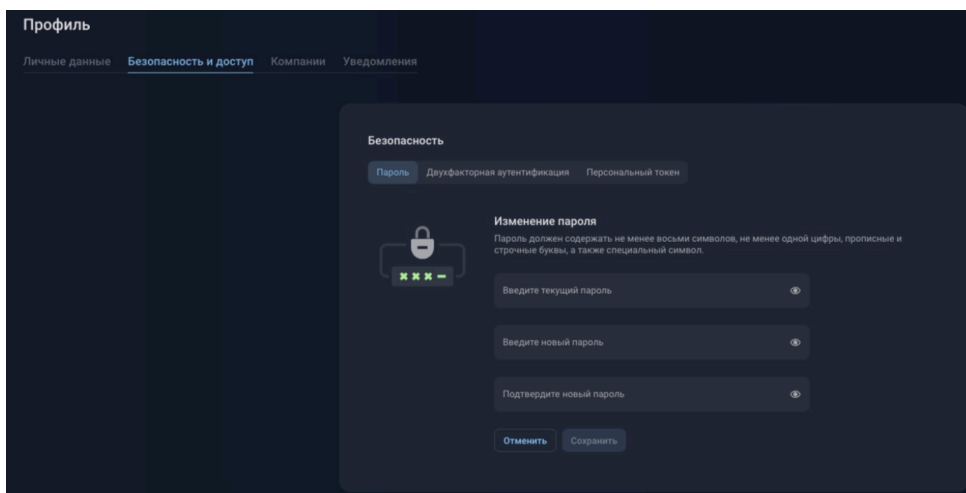
### Безопасность

В разделе "Безопасность" доступны три категории: Пароль, Двухфакторная аутентификация и Персональный токен. В категории "Пароль" нажмите "Сменить пароль":

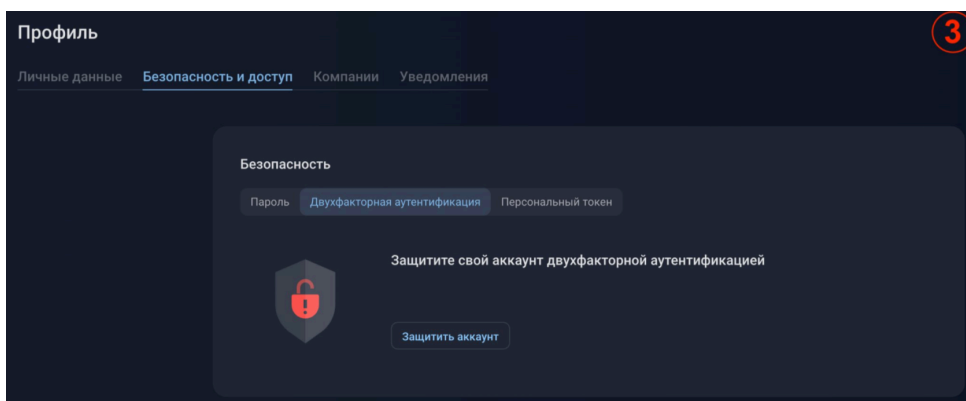


- Введите текущий пароль и создайте новый в соответствующих полях для ввода.

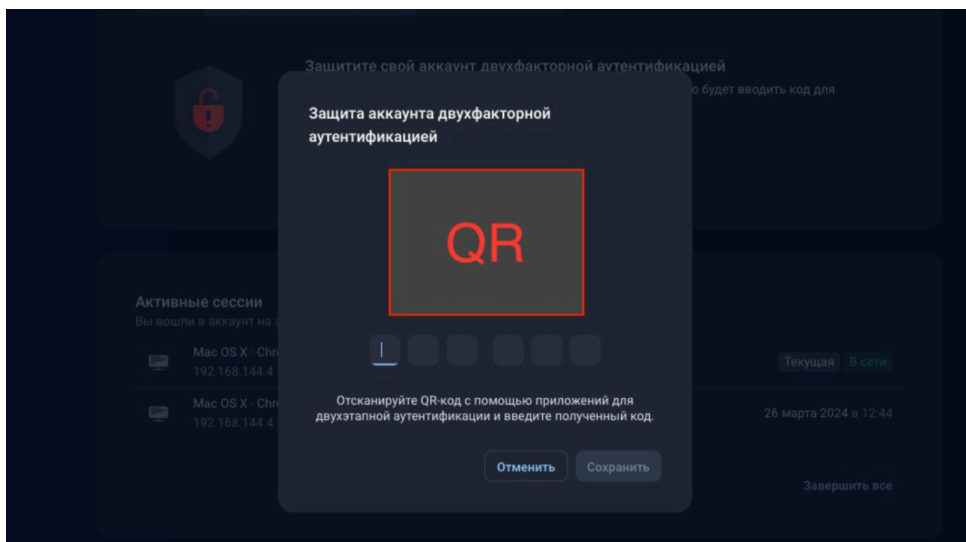
- После подтвердите новый пароль и сохраните изменения.



3. Для повышения безопасности учетной записи включите двухфакторную аутентификацию. Для этого перейдите в соответствующий раздел и нажмите "Защитить аккаунт".

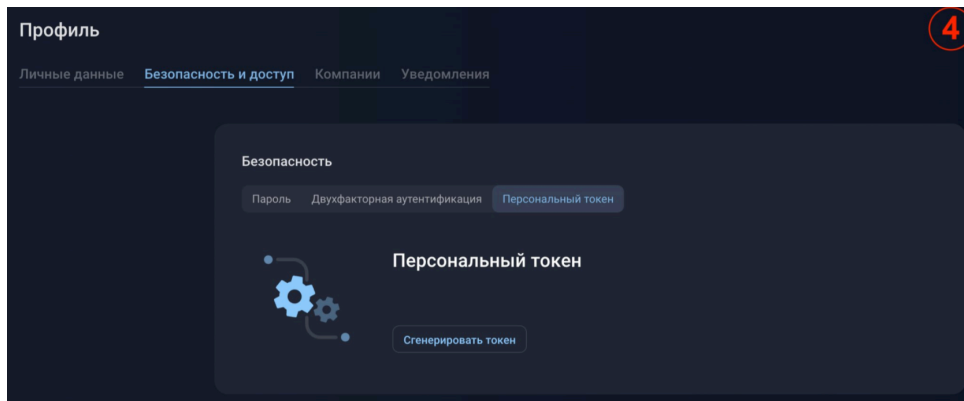


- В появившемся окне будет отображён QR-код.
- Скачайте приложение для двухфакторной аутентификации и отсканируйте этот QR-код.
- Затем введите полученный код в соответствующее поле.

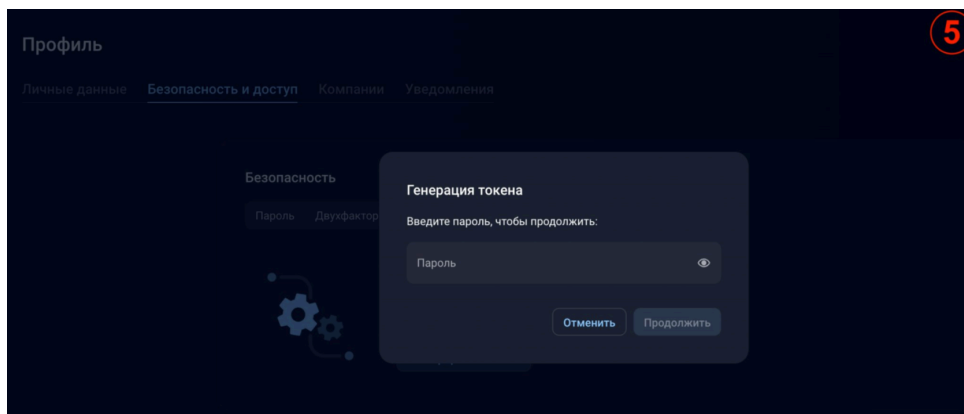


4. Для получения доступа к ресурсам и корректного взаимодействия с программным интерфейсом создайте свой персональный API-токен. Он служит для аутентификации и авторизации запросов, обеспечивая безопасность и контроль доступа.

- Перейдите в категорию "Персональный токен".
- Нажмите "Сгенерировать токен".

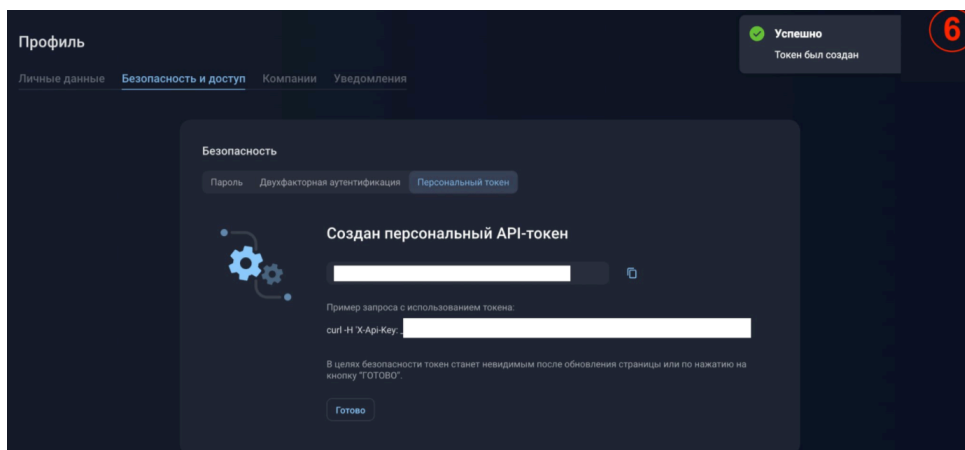


- Чтобы продолжить операцию, введите свой пароль.



После его подтверждения появится уведомление о успешном создании токена. В текущем окне будет отображен ваш персональный API-токен, который можно скопировать для дальнейшего использования.

- Ознакомьтесь с примером запроса, представленным ниже.
- Для завершения генерации токена нажмите кнопку "Готово".





## Уведомления

В разделе "Уведомления" представлен список типов уведомлений, которые вы можете получать на свой электронный адрес.

- Установите галочки и выберите уведомления, которые вы хотите получать.
- При желании укажите ключевые слова, касающиеся интересующих вас уведомлений.
- После выбора типов уведомлений и ввода ключевых слов, не забудьте сохранить все изменения.

Профиль

Личные данные Безопасность и доступ Компании Уведомления

**Уведомления по почте**  
Выберите типы уведомлений, которые хотели бы получать по электронной почте. Для гибкой настройки можете использовать ключевые слова в поиске.

<input type="checkbox"/>	<input type="text"/>	Поиск
<input type="checkbox"/>	<input type="text"/>	Поиск
<input type="checkbox"/>	<input type="text"/>	Поиск
<input checked="" type="checkbox"/>	<input type="text"/>	Поиск
<input checked="" type="checkbox"/>	<input type="text"/>	Поиск
<input type="checkbox"/>	<input type="text"/>	Поиск
<input type="checkbox"/>	<input type="text"/>	Поиск
<input type="checkbox"/>	<input type="text"/>	Поиск
<input checked="" type="checkbox"/>	<input type="text"/>	Поиск
<input type="checkbox"/>	<input type="text"/>	Поиск
<input type="checkbox"/>	<input type="text"/>	Поиск
<input checked="" type="checkbox"/>	<input type="text"/>	Поиск
<input type="checkbox"/>	<input type="text"/>	Поиск

