Контроль прав доступа

Задание 1.

Необходимо провести аудит учётных записей сотрудников некредитной финансовой организации в соответствии с применимыми (определить самостоятельно) регуляторными требованиями. Выявить нарушения, если таковые имеются и предложить корректирующие меры.

Дополнительно: составить SQL-запрос или PowerShell-скрипт для автоматизированного выявления неиспользуемых (более 90 дней) учётных записей.

Login	IsActive	CreateDate	LastLogOnDate	CurrentDate	Owner	IsLeaver
Ivanov	1	2022-05-12	2025-02-28	2025-03-01	Ivanov Ivan	0
Petrov	1	2021-03-15	2024-12-27	2025-03-01	Petrov Petr	0
Sidorov	0	2020-01-10	2025-02-27	2025-03-01	Sidorov Ruslan	0
test_user	1	2025-02-28	2025-03-01	2025-03-01	#N/A	#N/A
Semenov	0	2023-07-02	2025-02-28	2025-03-01	Semenov Sergey	1
CRM_admin	1	2021-01-01	2025-03-06	2025-03-01	Ivanov Ivan	0
CRM_integration	1	2025-01-20	2025-03-01	2025-03-01	Petrov Petr (tech account)	0
Sukhov	1	2024-11-10	2025-03-01	2025-03-01	Sukhov Alex	1

Есть некоторые нарушения по некоторым требованиям: 149-ФЗ «Об информации, информационных технологиях и о защите информации»; 152-ФЗ «О персональных данных», Требования по защите коммерческой тайны (98-ФЗ); Требования по защите инсайдерской информации (224-ФЗ); Требования по защите данных в Национальной платежной системе (161-ФЗ, ПП-584, 382-П и другие); ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций; Национальный стандарт РФ ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»; РС БР ИББС-2.9-2016 «Предотвращение утечек информации».

Нарушение 1: некоторые имена учётных записей с сомнительными названиями. В данной таблице некоторые имена учётных записей имеют странные названия: test_user, CRM_admin и CRM_integration. Учётную запись test_user не стоит использовать в базе данных, которая содержит реальные персональные данные, а её можно использовать для проведения различных SQL тестов и после их проведения удалить его.

Учётные записи CRM_admin и CRM_integration будут атакованы в первую очередь, поскольку они буквально обозначают их названия, роли и полномочия, так что они будут крайне легко скомпрометированны. Самое главное это убрать такие учётные записи и не добавлять их с такими названиями, в бизнесе стоит их называть по реальным именам и фамилиям. Переназначить права на другие учётные записи в случае если они будут удалены.

Нарушение 2: у учётной записи CRM_admin последняя дата в поле LastLogOnDate входа опережают текущую дату в поле CurrentDate. У данной учётной записи указано, что последняя дата входа составляет 6 марта 2025 года, хотя текущая дата 1 марта 2025 года. Поменять последнюю дату входа поле LastLogOnDate на настоящую, но главное чтобы она не опережала текущую дату из поля CurrentDate.

Нарушение 3: у имени владельца учётной записи CRM_integration лишняя пометка. У владельцев других учётных записей нету никаких пометок, но у владельца учётной записи CRM_integration есть пометка, что это технический аккаунт. Её стоит убрать, чтобы другие не узнали.

Нарушение 4: у учётных записей Sukhov и Sidorov одинаковые значения у полей IsActive и IsLeaver. У учётной записи Sukhov в полях IsActive и IsLeaver значение 1, а у учётной записи Sidorov 0. Учётные записи не могут одновременно быть активными и неактивными в системе. Поменять значение в полях IsActive и IsLeaver у обоих учётных записях, если они оба неактивны, то у поля IsLeaver поменять на 1 и IsActive на 0 и наоборот.

```
postgres=# SELECT d.directory_name AS "Directory",
    u.user_name AS "Username",
    to_timestamp(CAST(ca.attribute_value AS BIGINT)/1000) AS "Last Login"
FROM cwd_user u
    JOIN cwd_directory d ON u.directory_id = d.id
    LEFT JOIN cwd_user_attributes ca ON u.id = ca.user_id AND ca.attribute_name = 'login.lastLoginMillis'
WHERE u.active = 1
    AND d.active = 1
    AND u.lower_user_name IN (
            SELECT DISTINCT lower_child_name
            FROM cwd_membership m
            JOIN licenserolesgroup gp ON m.lower_parent_name = lower(gp.GROUP_ID))
    AND (u.id, u.directory_id) IN (
            SELECT ca.user_id, u.directory_id
            FROM cwd_user_attributes ca
            JOIN cwd_user u ON ca.user_id = u.id
            WHERE attribute_name = 'login.lastLoginMillis' AND to_timestamp(CAST(ca.attribute_value as bigint)/1000) <=
current_date - 90
            AND u.directory_id IN (
                SELECT id FROM cwd_directory WHERE active = 1))
    AND (u.id, u.directory_id) NOT IN (
            SELECT ca.user_id, u.directory_id
            FROM cwd_user_attributes ca
            JOIN cwd_user u ON ca.user_id = u.id
            WHERE attribute_name = 'login.lastLoginMillis'
            AND u.directory_id IN (
                SELECT id FROM cwd_directory WHERE active = 0))
ORDER BY "Last Login" DESC;
ERROR:  relation "cwd_user" does not exist
LINE 4: FROM cwd_user u
             ^
postgres=#
```

Данный SQL-запрос выглядит примерно вот так.

Задание 2.

В Компании используется следующая система аутентификации:

► Парольная аутентификация с минимальными требованиями: длина пароля от 6 символов, обязательные цифры и буквы.

► Политика смены паролей раз в 30 дней.

► Блокировка учётных записи после 5 неудачных попыток входа в течение 10 минут.

► Отсутствует двухфакторная аутентификация (2FA).

Определите основные уязвимости данной системы и объясните, какие риски они несут. Разработайте рекомендации по улучшению аутентификации и парольной политики.

Дополнительно: предложите оптимальную стратегию аутентификации для Компании среднего размера (500 сотрудников), учитывая баланс между безопасностью, удобством и затратами. Обоснуйте свой выбор.

1 уязвимость: длина пароля и используемые символы. В данной системе аутентификации недостаточное количество используемых символов. Несмотря на то, что такие требования для пароля удобны персоналу компании, но хакеры смогут взломать эти лёгкие пароли через brute force за несколько секунд (или секунду), и тогда хакер сможет делать всё что угодно с скомпрометированным аккаунтом. Для более надёжной защиты пароль должен состоять как минимум из 16 символов, также помимо букв и цифр обязательно использоваться различные символы. Такие пароли сложнее скомпрометировать и у хакера могут занять годы на их взлом через brute force. Дополнительно пароли могут быть уникальными (на каждый аккаунт используется совсем другой пароль), поскольку использовав один пароль на нескольких аккаунтах, скомпрометировав его будут скомпрометированы другие аккаунты с его использованием. Могут использоваться пароли словосочетания, которые относительно легко запомнить, но трудно взломать хакеру (пароль может состоять из 6 слов). Для того, чтобы хранить все эти пароли — у компании должен быть свой менеджер паролей, работникам достаточно знать один пароль для входа в менеджер паролей.

2 уязвимость: отсутствие двухфакторной аутентификации (2FA). Несмотря на то, что минимальные требования пароля были усилены, хакеры могут найти способ обойти пароль. В случае если хакер знает данные для входа в скомпрометированный аккаунт, то он сможет в него спокойно войти. Двухфакторная аутентификация сможет усложнить компроментацию аккаунта.

При введении имя пользователя/э.почту и пароль, настоящему владельцу аккаунта придёт уведомление с 4/5-значным кодом подтверждения входа в аккаунт. Даже если хакер знает данные для входа в аккаунт, то он не сможет спокойно ввойти, поскольку он не узнает код подтверждения. Двухфакторную аутентификацию необходимо включать, привязав аккаунт через специальное приложение для двухфакторной аутентификации или использовать номер телефона для получения одноразового кода подтверждения.

3 уязвимость: отсутствие системы IAM (Identity and Access Management). Даже если в компании имеются правила касаемо прав доступа, среди работников могут оказаться те, которые могут использовать свои права доступа для совершения подозрительных действий. В любой компании, в которой есть отдел по кибербезопасности, система IAM (Identity and Access Management) необходима для современных организаций. Система IAM (Identity and Access Management) является комплексом политик, процессов и использованных технологий. С её помошью можно назначать роли авторизованных пользователей, контролировать доступ пользователей к данным, мониторить активность для защиты чувствительных данных и предотвращать несанкционированные действия.

Для оптимальной стратегии аутентификации необходимо создать оптимальную систему IAM (Identity and Access Management). Она будет состоять из 5 важных компонентов:

1. Single Sign-On (SSO): Такая система позволяет войти на несколько аккаунтов/сервисов набрав логин и пароль один раз. Снижает затраты и нагрузку на IT ресурсы, не требует много паролей, снижает риск утечек, делает систему более удобной.

2. Аудит и отчитывание об исполнение (Audit and Compliance Reporting): Необходимая часть системы, которая во время проведения аудита или проверки со стороны проверяющих организаций помогает генерировать отчёты со всеми необходимыми данными, а также помогать исполнять требования по информационной безопасности, например GDPR.

3. Двухфакторная аутентификация (2FA): Система 2FA генерирует одноразовый код для подтверждения входа пользователя в аккаунт, после того когда были набраны логин и пароль от него. Делает систему в целом более безопасной, но менее удобной для персонала.

4. Привилегированный контроль доступа (Privileged Access Control): Важный компонент системы, у каждого пользователя назначаются разные полномочия и права доступа, чтобы пользователи не смогли повредить критические компоненты системы.

5. Контроль данных (Data Governance): процесс который позволяет контролировать доступность, целостность, безопасность и используемость данных. Это включает используемость политик и стандартов об использовании данных, чтобы убедиться что используемые данные являются достоверными и не использовались где не нужно.

Персональные данные

Задание 1.

Условие:

Компания планирует запустить новый сайт для размещения информации о свободных вакансиях и программах стажировок, а также приёма анкет и резюме от пользователей (соискателей). Планируется, что пользователь будет регистрировать на сайте личный кабинет (по электронной почте и номеру телефона) и с помощью него откликаться на вакансии и направлять резюме. Также с помощью личного кабинета пользователь сможет управлять подпиской/отпиской на рассылки Компании о новых вакансиях и стажировках. С помощью сайта Компания также хочет собирать техническую информацию о поведении пользователей (время пользовательской сессии; тип устройства пользователя; разделы, которые посещал пользователь и тп.)

Компания зарегистрирована и работает в РФ, целевыми пользователями нового сайта также являются граждане РФ.

Вопрос 1: Какие обязательные функции/разделы/информация по вашему мнению должны быть на сайте, чтобы Компания не нарушала требований законодательства РФ?

На публичной части сайта может быть использована следующая информация: номер телефона и электронная почта, для обработки технической поддержкой вопросов от пользователей. Во время создания новой учётной записи, пользователь обязан давать согласие на обработку персональных данных по закону ФЗ-152. На подразделе о вакансии сайта в контактах могут содержаться контактные данные рекрутера (электронная почта/номер телефона и ФИО рекрутера), название самой компании и его логотип. Сайт может состоять из разделов о странице с предлагаемыми вакансиями, поисковиком, новостями, статистике, о самой компании, профилем пользователя, а в самом профиле возможность создать/изменить резюме или использовать готовое резюме. В административной части сайта определённые работники имеют разные полномочия и определённый доступ к инструментам и их функциям, для модерации контента, добавления и удаления данных и пользователей. Может использоваться инструмент для генерирования отчётов, при запросах отправлять данные в нужные органы.

Вопрос 2: Вам нужно понять насколько хорошо будут защищены пользовательские данные, которые собирает сайт. Какие вопросы Вы бы задали представителям Компании, чтобы это понять?

Какой уровень защиты информации у Вас используется (от D до A)? Насколько часто у Вас проходят проверки на соответствие с требованиями законодательства?

Какие комплексы технологий и механизмов безопасности используются для защиты информации (вроде DLP, IAM или NGFW)? Используется ли у Вас политика Zero Trust? В каком формате хранится собранная на данном сайте информация? Имеется ли у данного сайта безопасное подключение (https)? Как часто у Вас обновляют программное обеспечение? Через какое время Вы удаляете информацию, в случае если пользователь перестал пользоваться услугами сайта или когда пользователь подаёт запрос на её удаление? Как часто у Вас проводят лекции на повышение осведомлённости персонала об новых рисках информационной безопасности? Какой у Вас алгоритм действий в случае начала инцидента (вроде начала кибератаки)? Как часто у Вас проходит инвентаризация?

Задание 2.

Условие:

В компанию обратился клиент с запросом об удалении всех его персональных данных из всех информационных систем Компании. Клиент обосновал свой запрос тем, что качество продукции и клиентского сервиса сильно снизились. Клиент также пригрозил обращением в суд в случае если компания не выполнит его требования.

Примечание: До этого клиент долгое время пользовался услугами Компании, покупал её продукцию, участвовал в акциях и программах лояльности.

Вопрос 1: Должна ли компания удовлетворить запрос клиента и полностью удалить все его персональные данные из всех своих информационных систем? Аргументируйте вашу позицию.

Изначально стоит проверить активность клиента, если он был действительно был активен до предъявления запроса, то стоит вежливо отклонить запрос данного клиента, поскольку по данным ФЗ-152, персональные данные нельзя удалить сразу, а только через 30 дней в случае одобрения запроса. Чтобы его запрос одобрили, ему необходимо предоставить свои персональные данные, а также перечень данных, которые требуется удалить или запретить передавать третьим лицам. С момента поступления запроса от клиента, прекращается обработка персональных данных в течение 3 рабочих дней, но не их удаление. В случае если суд удовлетворит запрос клиента, то нужно удалить персональные данные в течение 3 рабочих дней.

Вопрос 2: Попробуйте составить официальный ответ на запрос клиента.

Мы сможем удовлетворить Ваш запрос, но по закону мы не можем удалить Ваши данные сразу. Для удовлетворения запроса заполните анкету, а также не забудьте указать перечень персональных данных, которые Вы хотите удалить. Ваши данные будут удалены в течение 30 рабочих дней, но они не будут передаваться третьим лицам.

Задание 3.

Компания хочет создать новую систему, с помощью которой будет вестись учёт всех клиентских обращений. В системе будут содержаться:

- информация о пользователях, направивших обращение (ФИО, контактные данные)
- информация о содержании самих обращений/статусе их рассмотрения
- информация о способе получения обращения (по телефону/эл.почте/в письменном виде/в мессенджере/на сайте)

Компания будет сама заниматься разработкой и запуском системы, не привлекая для этого сторонние организации. Доступ к системе будет только у сотрудников Компании.

Вопрос: Какие рекомендации в части информационной безопасности и защиты персональных данных Вы бы дали коллегам на этапе проектирования системы? По возможности аргументируйте свои ответ ссылками на законодательство РФ.

В области информационной безопасности: рекомендовано разграничить права доступа для ответственных за внесение/удаление/изменение данных; во время проектирования также необходимо проводить тестирование на проникновение и сканирование на уязвимости и составить отчёт о проведённых тестах; использовать только самые необходимые сетевые порты (например 22 и 443) или переназначить некоторые сетевые протоколы на другие порты (например 22 порт сменить на 2222 порт) используя огненную стену/фаервол, установить другие технологии безопасности — вроде IDS/IPS, SSO, NGFW, AV, etc.

В области защиты персональных данных: главное чтобы раздел с персональными данными не был виден на публичной части сайта, а также не было никаких подразделов, которые могут привести в административную часть; внедрить систему DLP (Data Leak Prevention) для сканирования на конфиденциальную информацию; обязательно должна быть функция об подтверждении обработки персональных данных.

Security Operations Center

Сотрудник Компании пожаловался на получение подозрительного письма, отправитель которого ему неизвестен.

Вопрос 1: Какие действия необходимо предпринять?

Не стоит нажимать на ссылку, поскольку в большинстве случаев ссылки из подозрительных писем в большей степени содержат вредоносы или вредоносные файлы. Далее необходимо проанализировать содержимое данного письма, в случае с ссылкой необходимо проверить её безопасность. Если при нажатии по ссылке устанавливается простой файл, нужно проверить его внутренности, чтобы убедиться что в нём нету вредоносного кода.

Вопрос 2: На что обратить внимание при анализе?

В первую очередь нужно обратить внимание на почтовый адрес отправителя и на его никнейм, поскольку могут быть некоторые пользователи, которые не используют реальные имена в качестве имени отправителя, но также стоит проверить всё содержимое письма для анализа его контекста.

Предотвращение утечек информации (DLP)

Вопрос 1: Как расшифровывается аббревиатура DLP? Какие основные задачи решает направление предотвращение утечек данных? Каналы утечки информации и способы защиты.

DLP расшифровывается как Data Leak Prevention. Главное в направлении предотвращения утечек данных это оценивать риски, чувствительность информации, обнаруживать каналы по которым может произойти утечка данных и блокировать их. Данные могут утечь по многим каналам: переносимые хранилища (USB, флэшки и др.) э.почта, мессенджеры, социальные сети, платформы для обмена файлов, веб-сайты и др. Также данные могут утечь из вне и изнутри. Для защиты от утечек необходимо блокировать все возможные каналы, запрещять приносить переносные устройтсва, выносить устройства из компании содержащие чувствительную информацию, проводить периодические проверки, мониторить всю активность.

Вопрос 2: Что такое DLP-система? Какой функционал она обеспечивает?

DLP-система это система для идентификации, отслеживания и охраны конфиденциальной и чувствительной информации он несанкционированного доступа. DLP-система сканирует всю информацию в установленном сегменте системе и блокирует все возможные попытки нарушения политик DLP установленные в системе и сообщения, которые содержат чувствительную информацию.

Вопрос 3: Какую роль играют регулярные выражения в DLP-системе? Приведите примеры их применения.

Регулярные выражения помогают искать не только специфический текст, но и текстовые паттерны, это более точный способ поиска чувствительной информации. С помощью регулярных выражений можно обнаружить чувствительную информацию в неожиданных местах/каналах (например неверно сконфигурированный файл).

Вопрос 4: Контекстным анализом проще идентифицировать номер телефона РФ в документе, чем ФИО. Верно ли утверждение и почему?

Данное утверждение является верным, поскольку с помощью контекстного анализа система DLP можно проанализировать содержимое документа(ов) на конфиденциальную информацию не рассматривая её вручную. Можно создавать политики, которые будут учитывать все важные атрибуты среды, в которой конфиденциальная информация существует.

Вопрос 5: Вы проводите стажировку в компании «Феникс», к вам обращается руководитель отдела продаж и сообщает, что подозревает сотрудника Петрова в попытках выгрузить за периметр Компании базу клиентов. Ваши действия?

Сначала проанализировать в DLP-системе на возможные нарушения политики DLP, в том числе с использованием регулярных выражений, проанализировать всю активность учётной записи сотрудника Петрова, а также проверить всевозможные каналы, по которым может произойти утечка данных и спросить у данного сотрудника по поводу различных переносных хранилищ и других подозрительных для DLP предметов. В случае если данный сотрудник действительно пытался вывести базу клиентов за периметры компании, то предупредить его об юридических, финансовых и репутационных последствиях и наказать его за нарушение закона №152-ФЗ о персональных данных, за попытку утечки данных.

Практическое задание:

Регулярное выражение для поиска адреса электронной почты.

Регулярное выражение для поиска любой электронной почты:

(?:^|\s)[\w!#$%&'*+/=?^`{|}~-](\.?[\w!#$%&'*+/=?^`{|}~-])*@\w+[.-]?\w*\.[a-zA-Z]{2,3}\b

Регулярное выражение для поиска электронной почты со специфическим доменом:

(?:^|\s)[\w!#$%&'*+/=?^`{|}~-](\.?[\w!#$%&'*+/=?^`{|}~-])*@company.com

Безопасность приложений (Application Security)

Задание 1:

Условие:

На компьютере пользователя происходит срабатывание антивирусной защиты.

Вопрос 1: Какие действия необходимо предпринять для проверки на ложноположительное срабатывание?

В случае когда сработало ложноположительное срабатывание, самое главное это не подтверждать и не удалять такие файлы до тех пор, пока не появится больше информации. Другие действия: просканировать с помощью VirusTotal; отправить неизвестные файлы на карантин для дальнейшего анализа; сообщить антивирусному провайдеру.

Вопрос 2: В случае, если это реальный вирус, то какие действия необходимо предпринять для оценки поверхности атаки и распространения?

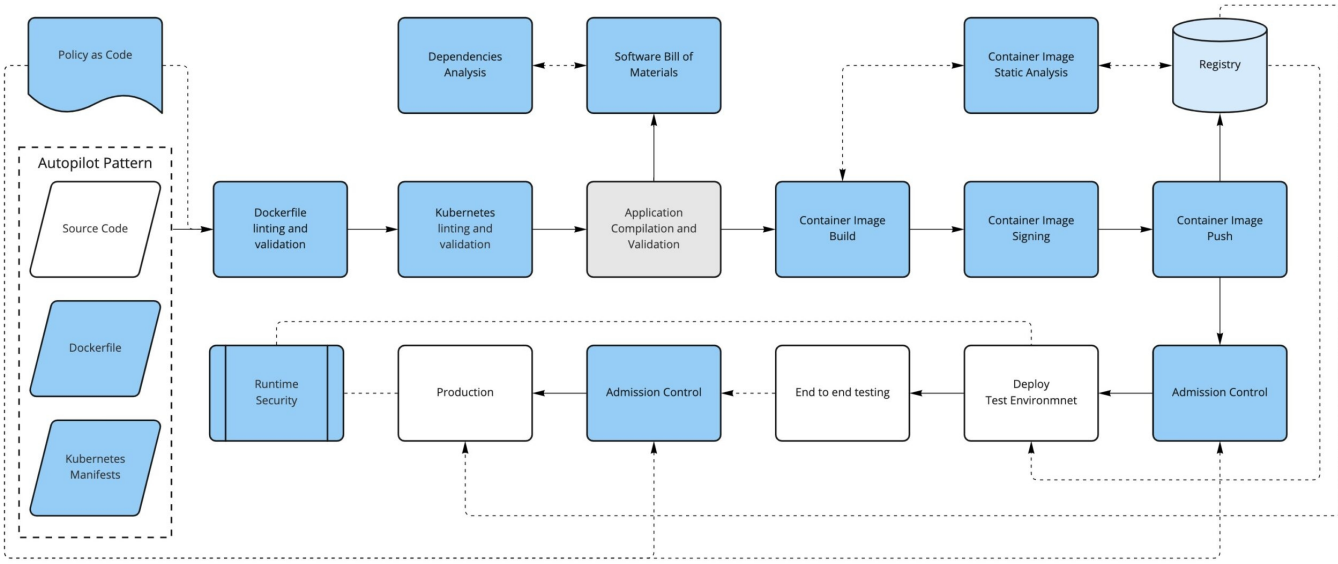
Отправить данный файл на карантин для дальнейшего анализа; проанализировать его с помощью утилит(ы) для просмотра содержимого кода самого файла; в случае если компания использует свой антивирус — внести данный файл в базу данных вредоносов; проверить свойства файла.

Задание 2:

Условие:

В Компании разрабатывается собственные программные продукты на языке Java с применением GitLab CI/CD и сборкой через Gradle. Перед Вами стоит задача предложить контроли безопасности по проверке исходного кода, зависимостей и инфраструктуры будущего приложения (Docker, Kubernetes).

Вопрос 1: Опишите или нарисуйте пайплайн сборки и доставки в общих чертах с включёнными проверками кода.



Данный пайплайн выглядит примерно вот так.

Вопрос 2: Почему Вы выбрали такие решения?

С помощью такого пайплайна будет более безопасная проверка кода при продолжительном цикле DevSecOps.

Вопрос 3: Какие образом будут осуществляться контроль работы проверок и их результат?

В цикле DevSecOps используются технологии безопасности: Static Application Security Testing (SAST), Secrets detection, Software Composition Analysis (SCA), Cloud Security Posture Management (CSPM) и др.

Задание 3:

Условие:

У вас есть список IP-адресов обращений к ресурсу компании, например:

- 185.12.30.76
- 213.209.133.185
- 15.204.40.211
- 89.113.144.217
- 188.170.177.78
- 83.217.200.199
- 213.186.1.154
- 31.10.97.225
- 146.185.196.19
- 94.247.111.51
- 128.204.77.80
- 5.255.231.149
- 113.20.159.50
- 79.134.203.30
- 92.38.128.71

Задача:

Написать код, который соберёт отдельные IP-адреса в подсети, обратится к ресурсу https://ip-api.com и достанет имя провайдера и страну, запишет подсеть провайдера и страну в любую базу данных на Ваше усмотрение.

```
import requests
import pandas as pd

ips = ['185.12.30.76', '213.209.133.185', '15.204.40.211', '89.113.144.217', '188.170.177.78',
'83.217.200.199',
       '213.186.1.154', '31.10.97.225', '146.185.196.19', '94.247.111.51', '128.204.77.80', '5.255.231.149',
       '113.20.159.50', '79.134.203.30', '92.38.128.71']
response = requests.post("http://ip-api.com/batch", json=ips).json()
response = pd.DataFrame(response)
print(response)
```

Код выглядит примерно вот так.

P.S. В реальности я бы использовал лист с IP-адресами и домен API в отдельных файлах.