Урок 3. Интернет и безопасность данных (GDPR)

Интернет

Интернет - это глобальная сеть компьютеров, соединенных между собой, которая позволяет обмениваться информацией и данными по всему миру.

Представляет собой множество сетей, объединенных в единую сеть.
Предоставляет доступ к различным ресурсам: веб-сайтам, электронной почте, файлам, мультимедийному контенту и т.д.

Интернет состоит из трех физических компонентов:

- среды передачи данных (провода, кабели, радиоволны)
- маршрутизаторов
- сетей

Интернет-инфраструктура - сочетание интернет-оборудования и программного обеспечения, которое на нем работает.

Среда передачи - данные могут передаваться по проводам, оптоволоконному кабелю или в беспроводной сети (например, вай-фай).

Маршрутизаторы - устройства, определяющие оптимальный маршрут для передачи данных, которые могут передаваться по нескольким маршрутам.

Сети - компьютеры и мобильные устройства подключаются к небольшим сетям (соединяются между собой).

Для обмена данными за пределами этих сетей требуется поддержка интернет-провайдера (ISP). Интернет-провайдер предоставляет такой доступ в интернет и иную поддержку, связанную с работой в интернете.

История интернета

Краткий обзор истории возникновения и развития интернета:

Предпосылки (1950-1960-е годы):

- Концепция связи между компьютерами возникает еще в 1950-х годах.
- В 1960-х годах в США начинаются исследования в области коммуникаций и компьютерных сетей.

Первые шаги к созданию интернета (1960-1970-е годы):

- В 1969 году американский ученый Леонард Клей реализует первую успешную передачу данных между компьютерами в рамках проекта ARPANET (Advanced Research Projects Agency Network).
- В 1971 году появляется электронная почта.
- Термин "Интернет" и развитие сетей (1980-е годы):
- В 1983 году термин "Интернет" (Internet) официально становится обозначением для сети сетей.
- В 1985 году создается доменная система DNS (Domain Name System), что делает адресацию ресурсов в Интернете более удобной.

 **DNS (система доменных имен) - это система, используемая в компьютерных сетях для преобразования человеко читаемых доменных имен, таких как microsoft.com, в числовые IP-адреса, которые используются компьютерами для обмена данными.**

 **URL (Uniform Resource Locator) - это адрес, который определяет местоположение ресурса (например, веб-страницы, файла, изображения или другого типа контента) в интернете.**

URL используется для обозначения точного пути к ресурсу и позволяет пользователям и программам легко находить и получать доступ к этому ресурсу.

 **Пример:**

Когда вы вводите URL (Uniform Resource Locator) в веб-браузере, например, "www.example.com", ваш компьютер отправляет запрос на разрешение доменного имени (DNS-запрос) к DNS-серверу. DNS-серверы содержат базы данных соответствий доменных имен и IP-адресов. DNS-сервер выполняет преобразование доменного имени "www.example.com" в соответствующий IP-адрес.

Затем ваш компьютер может использовать полученный IP-адрес, чтобы установить соединение с веб-сервером, хранящим содержимое сайта "www.example.com". Это позволяет браузеру загрузить и отобразить веб-страницу.
DNS играет важную роль в интернете, обеспечивая удобство использования человеко читаемых доменных имен вместо запоминания сложных числовых IP-адресов. Без DNS было бы гораздо сложнее использовать интернет, поскольку пользователю пришлось бы помнить IP-адреса каждого веб-сайта, который он хочет посетить.

Коммерческое развитие интернета (1990-е годы):

- В 1990 году Тим Бернерс-Ли представляет WWW (World Wide Web) - систему гипертекстовых ссылок, что становится основой современного интернета.
- В 1991 году начинается коммерческое использование интернета.
- В 1994 году появляется первый коммерческий браузер Netscape Navigator.
- Развитие и распространение интернета в мире (2000-е годы):
- В 2000-х годах интернет становится всеобщим явлением, доступным для широкой аудитории.
- Появляются социальные сети, видеохостинги, онлайн-платформы для образования и многое другое.
- Быстрое развитие технологий и повышение скорости интернет-соединений.

Браузер (иногда также называемый веб-браузером) - это программное обеспечение, которое позволяет пользователям просматривать, получать доступ и взаимодействовать с веб-сайтами, а также отображать различные типы веб-контента, такие как текст, изображения, видео и аудио.

Основная функция браузера - предоставить пользователю удобный интерфейс для работы с интернетом. Когда пользователь вводит URL (Uniform Resource Locator) или кликает на ссылку, браузер отправляет запрос на сервер, хранящий запрошенную веб-страницу. Затем браузер загружает и отображает содержимое страницы на экране пользователя. Современные браузеры имеют множество дополнительных функций, таких как поддержка вкладок, возможность сохранения паролей, добавление расширений и плагинов, защита от вредоносных программ и многое другое. Популярные браузеры:
Google Chrome, Mozilla Firefox, Microsoft Edge, Safari и другие.

Современный интернет (2010-е годы и далее):

- Интернет становится неотъемлемой частью повседневной жизни, оказывая влияние на все сферы общества.
- Развивается интернет вещей (IoT), искусственный интеллект, облачные вычисления и другие передовые технологии.

- Концепция Интернета 5G, обеспечивающего более высокую скорость и надежность соединения, становится реальностью.
- История интернета связана с постоянным развитием и инновациями, что делает его одним из самых важных достижений современной цифровой эпохи.

Задание для закрепления

1. Какая система гипертекстовых ссылок стала основой современного интернета?
    a. WWW (World Wide Web)
    b. ARPANET (Advanced Research Projects Agency Network)
    c. DNS (Domain Name System) d) IoT (Internet of Things)
2. В каком году началось коммерческое использование интернета?
    a. 1950 год
    b. 1971 год
    c. 1985 год
    d. 1991 год
3. Какая технология обеспечивает более высокую скорость и надежность соединения в современном интернете?
    a. Интернет вещей (IoT)
    b. Искусственный интеллект
    c. Интернет 5G

Интернет - протоколы

Протокол - это набор правил и соглашений, определяющих формат и последовательность обмена данных между устройствами в компьютерных сетях.

Протоколы обеспечивают стандартизацию взаимодействия между устройствами и позволяют им эффективно обмениваться информацией, таким образом, обеспечивая согласованность и надежность передачи данных.

Роль протоколов в обеспечении передачи данных между устройствами в сети:

- Установление соединения: Протоколы определяют процедуры установления соединения между устройствами, позволяя им установить связь и начать обмен данными.
- Формат данных: Протоколы определяют формат данных, который должен быть соблюден для правильной передачи информации между устройствами.
- Управление потоком данных: Протоколы регулируют передачу данных, контролируя скорость передачи, обнаруживая и исправляя ошибки, а также контролируя доступ к сетевому каналу.
- Разделение и объединение данных: Протоколы могут разбивать большие блоки данных на более мелкие (пакеты) для передачи и объединять их обратно на стороне получателя.
- Маршрутизация: Некоторые протоколы также обеспечивают определение пути, по которому будут передаваться данные между устройствами.
- Обнаружение ошибок: Протоколы предусматривают механизмы для обнаружения и исправления ошибок, возникающих в процессе передачи данных.
- Завершение соединения: После завершения обмена данными, протоколы предусматривают процедуры для корректного завершения соединения между устройствами.

Благодаря протоколам возможно согласованное взаимодействие устройств в сети, обеспечивая надежность, эффективность и безопасность передачи данных между компьютерами и другими сетевыми устройствами.

Веб-сервер - это программное обеспечение или компьютер, который хранит веб-сайты и обеспечивает их доставку пользователям через интернет.

Он играет ключевую роль в клиент-серверной архитектуре интернета.

Популярные протоколы:

- HTTP (Hypertext Transfer Protocol): HTTP является протоколом прикладного уровня, используемым для передачи данных между клиентами и веб-серверами во Всемирной паутине. Этот протокол поддерживает запросы клиента к серверу (например, запрос на получение веб-страницы) и ответы сервера на эти запросы (например, передача запрошенной веб-страницы).
  Пример использования HTTP: Когда вы открываете свой веб-браузер и вводите URL-адрес сайта, ваш браузер отправляет HTTP-запрос на веб-сервер, который содержит запрос на получение веб-страницы. Затем сервер отправляет HTTP-ответ с содержимым веб-страницы, которую вы видите на своем экране.
- TCP/IP (Transmission Control Protocol/Internet Protocol): TCP/IP - это семейство протоколов, которые обеспечивают коммуникацию между устройствами в сети. Оно включает в себя ряд протоколов, таких как IP (Internet Protocol) для маршрутизации пакетов данных, TCP (Transmission Control Protocol) для обеспечения надежной передачи данных и другие.
  Пример использования TCP/IP: Когда вы отправляете электронное письмо, ваше устройство использует протокол TCP/IP для разбивки сообщения на пакеты данных и их отправки через сеть. Затем протоколы TCP/IP управляют передачей и повторной передачей пакетов, чтобы гарантировать, что ваше письмо успешно доставлено адресату.
- FTP (File Transfer Protocol): FTP - это протокол, используемый для передачи файлов между клиентами и серверами в сети. Он позволяет пользователям загружать и скачивать файлы на удаленный сервер.
  Пример использования FTP: Если у вас есть свой сайт и вы хотите обновить его содержимое, вы можете использовать FTP для загрузки новых файлов на веб-сервер. Это позволяет обновить содержимое вашего сайта без необходимости изменения его непосредственно на сервере.
- SMTP (Simple Mail Transfer Protocol): SMTP - это протокол, используемый для отправки и доставки электронных писем по электронной почте. Он отвечает за пересылку электронных писем от отправителя к почтовому серверу получателя.
  Пример использования SMTP: Когда вы отправляете электронное письмо, ваш почтовый клиент использует SMTP для отправки письма на почтовый сервер вашего провайдера. Затем SMTP-сервер отправляет письмо по сети к почтовому серверу получателя, который затем доставляет письмо в почтовый ящик адресата.

Сетевая модель OSI:

Теоретическая модель стека интернет-протоколов для взаимодействия устройств в сети была разработана в середине 70-х годов, как попытка стандартизации принципов работы сети.

В итоге не получила широкого применения на практике, но сегодня является наглядной образовательной моделью для изучения принципов работы сети.

Современный и актуальный интернет-стек на основе TCP/IP “вписывается” в модель OSI, то есть современные интернет-протоколы соответствуют определенным уровням модели OSI.

Модель позволяет понять, как данные от одного интернет-устройства передаются к другому и через какие трансформации они проходят (например, от текста в емейл-клиенте до электрических сигналов в проводах или световым потокам в оптоволокне). Также о модели по-прежнему иногда спрашивают на собеседованиях.

 **WWW - всемирная система публичных веб-страниц в сети Интернет. Сеть не является интернетом: сеть лишь использует интернет как среду передачи информации и данных.**

Это про обмен документов, связанных между собой гипертекстовыми ссылками. Идея принадлежит Тиму Бернерсу Ли, который придумал понятие URL для уникальной идентификации ресурсов (страничек) в сети, язык разметки гипертекста HTML и соответствующий протокол передачи документов HTTP.

После знакомства со стеком протоколов мы уже понимаем, что WWW может рассматриваться как часть интернета и реализована на верхнем, прикладном уровне модели OSI на основе протокола HTTP.

Документы во Всемирной паутине хранятся на специальных серверах, где запущен http-сервер. Самый популярный сервер сегодня - Apache http. Он умеет принимать запросы по протоколу HTTP и отвечать на них.

 **Пример:**

Когда вы пишите адрес сайта в строке браузера, то браузер отправляет http-запрос на удаленный http-сервер, который находится по этому адресу. Сервер принимает запрос и пытается его выполнить, например, ищет у себя запрашиваемую веб-страницу и, если она есть, отправляет ее содержимое обратно клиенту в

формате HTML. Ваш браузер понимает язык разметки HTML и отрисовывает страницу в понятном вам представлении.

Задание для закрепления

Соотнесите протокол и его назначение:

1. HTTP	A. Отправляете Email другу
2. TCP/IP	B. У вас есть свой сайт и вы хотите обновить его содержимое
3. FTP	C. Заходите на любимый сайт в браузере
4. SMTP	D. Скачиваете картинку с котиком из интернета

Клиент-серверная архитектура

Клиент-серверная архитектура - это модель взаимодействия между устройствами в сети, в которой компьютеры, называемые клиентами, обращаются к другим компьютерам, называемым серверами, для получения различных услуг, данных или ресурсов.

В этой модели клиенты и серверы выполняют разные роли и функции для обеспечения эффективного взаимодействия и передачи информации.

Клиент - это устройство или компьютер, которое инициирует запросы к серверу для получения данных или услуг.

Роль клиента:

- Клиент выполняет роль инициатора коммуникации и определяет тип запроса, который будет отправлен серверу.
- Клиент также ответственен за получение ответов от сервера и обработку полученных данных.

Примеры клиентов включают в себя веб-браузеры, почтовые клиенты, приложения для обмена сообщениями и другие программы, которые обращаются к серверам для получения данных или услуг.

Функции и задачи клиента:

- Инициирование запроса: Клиент инициирует взаимодействие, отправляя запрос серверу для получения данных или выполнения определенной задачи.
- Отправка данных: Клиент может отправлять данные на сервер для обработки или хранения. Например, отправка данных через веб-формы на сервер во время регистрации на сайте.
- Обработка ответа: Когда клиент получает ответ от сервера, он обрабатывает полученные данные и принимает решение о дальнейших действиях, основываясь на этой информации.
- Отображение данных: Клиент отображает данные, полученные от сервера, пользователю в удобном для восприятия формате. Например, отображение веб-страницы в браузере.
- Управление пользовательским интерфейсом: Клиент обеспечивает интерфейс, который позволяет пользователям взаимодействовать с приложением или сервисом на сервере.

Сервер - это устройство или компьютер, которое обрабатывает запросы от клиентов и предоставляет им необходимые данные, ресурсы или услуги.

Роль сервера:

- Сервер отвечает на запросы клиентов, обрабатывая их и предоставляя запрошенные данные или услуги.
- Серверы могут выполнять разнообразные функции, такие как хранение файлов, обработка данных, предоставление доступа к базам данных, хостинг веб-сайтов и другие.

Примеры серверов включают в себя веб-серверы, почтовые серверы, серверы баз данных и другие компьютеры, предоставляющие услуги и ресурсы клиентам.

Функции и задачи сервера:

- Прием запросов: Сервер принимает запросы от клиентов, анализирует их и определяет, какие действия должны быть выполнены.
- Обработка запросов: Сервер выполняет обработку запросов, выполняя необходимые операции, доступ к базам данных, вычисления и другие задачи, которые требуются для удовлетворения запросов клиентов.
- Отправка данных: Сервер отправляет ответы клиентам, содержащие запрошенные данные или результаты выполненных операций.
- Управление ресурсами: Сервер управляет доступом клиентов к ресурсам, таким как файлы, базы данных, процессорное время и память, чтобы обеспечить эффективное использование ресурсов системы.
- Безопасность: Сервер обеспечивает защиту данных и системы от несанкционированного доступа и злоумышленных действий.

Итак, “Клиент — сервер” — сетевая архитектура, в которой распределение нагрузки по выполнению задач распределено между поставщиками услуг, называемыми серверами и заказчиками (или потребителями) услуг, называемыми клиентами. В данном контексте сервер не обязательно физический компьютер, выполняющий задачи по заказу пользователя, но более широкое понятие поставщика услуг, которые предоставляются по запросу.

Пример:

Упрощенной аналогией из жизни может быть взаимодействие покупателя с магазином, где магазин-сервер предоставляет услуги по запросу покупателя-клиента. В интернет-мире сервером обычно является программа,

которая выполняет запрос программы-клиента, приходящий по сети в определенном формате, в соответствии с правилами протокола, о которых мы говорили выше. Например, почтовая серверная программа понимает запросы от ваших почтовых программ-клиентов на отправку ваших емейлов по протоколу SMTP.

Персональные данные пользователей в сети

Разрабатывая софтварные продукты, а также анализируя данные о поведении пользователей и компаний, вы, как инженер или дата-аналитик столкнетесь с персональными данными пользователей, заказчиков (частных лиц или компаний).

"Софтварные продукты" - это программные продукты или приложения, которые созданы для выполнения различных задач на компьютере или других устройствах.

Это понятие включает в себя программы, приложения, операционные системы, игры, утилиты и многое другое. Софтварные продукты разрабатываются для удовлетворения разнообразных потребностей пользователей, будь то работа, образование, развлечения или другие цели.

В разных странах приняты и работают различные законы, регулирующие работу с персональными данными пользователей. Не только владельцы бизнеса и ответственные менеджеры компаний должны понимать, какие законы применимы к их организациям и выстраивать бизнес-процессы, соответствующие легальным требованиям, но и дата аналитики и инженеры должны иметь представление о том, что является персональными данными и как с ними работать.

"Персональные данные пользователей" - это конфиденциальная информация, относящаяся к конкретным физическим лицам, которая может быть использована для их идентификации или связи с ними.

Эти данные могут включать в себя:

- Имя и фамилия: Основные личные данные, которые могут идентифицировать пользователя.
- Адрес электронной почты: Используется для связи и аутентификации.
- Номер телефона: Для связи и подтверждения личности.
- Адрес проживания: Место, где пользователь живет.
- Дата рождения: Используется для аутентификации и подтверждения возраста.
- Логин и пароль: Данные для доступа к аккаунту.
- Платежные данные: Информация о кредитных или дебетовых картах, используемых для онлайн-платежей.
- Информация о местоположении: Данные о географическом положении пользователя.

- Социальные профили: Информация из социальных сетей, которую пользователь размещает публично.
- Медицинская информация: Личные данные о здоровье и медицинской истории.
- Информация о работе: Данные о месте работы, должности и зарплате.

Персональные данные пользователей в сети требуют особой защиты, так как их утечка или несанкционированное использование может привести к серьезным нарушениям конфиденциальности и безопасности. Компании и организации, собирающие и обрабатывающие такие данные, должны следовать строгим нормам и законодательству, чтобы обеспечить их безопасность и соблюдение прав пользователей.

В онлайн-контексте персональные данные - это любая информация, которую пользователь предоставляет при регистрации на сайтах, использовании приложений, покупке товаров или услуг.

Это любая информация, относящаяся к идентифицированному или поддающемуся идентификации физическому лицу («субъекту данных», т. е. к человеку).

В контексте дата-аналитики речь обычно идет о потребителях услуг компании, на которую вы работаете. К таким данным могут относиться очевидные, как, например, емейл, имя и фамилия, адрес, так и менее очевидные данные пользователей, например, номер заказа или номер клиента в системе - в определенных обстоятельствах по таким номерам можно однозначно идентифицировать конкретного человека. соответственно, эти айдишники - персональные данные.

📎**"Айдишники" (или "IDшники") - это сокращенное название для термина "идентификаторы". В информационных системах и программировании идентификаторы используются для уникальной идентификации объектов, данных или пользователей.**

Они представляют собой уникальные значения, которые помогают различать один объект от другого.

В контексте программирования и баз данных, "айдишники" могут быть числами, строками или другими формами данных, которые уникально идентифицируют определенный объект. Например, в базе данных пользователей каждому пользователю может быть назначен уникальный числовой "айдишник", который будет использоваться для идентификации данного пользователя при выполнении

операций в системе. Это позволяет избежать путаницы и обеспечить корректную обработку данных.

Задание для закрепления

Что НЕ является персональными данными?

Зачем охранять персональные данные?

Пример:

Утечка медицинских данных пользователей, продажа баз данных номеров телефонов или продажа банковских транзакций.

Охрана персональных данных имеет критическое значение для защиты приватности, безопасности и прав граждан.

Основные причины, почему важно охранять персональные данные:

- Приватность: Охрана персональных данных обеспечивает право на приватность каждого человека. Люди имеют право контролировать, как их личная информация собирается, хранится и используется.
- Предотвращение злоупотреблений: Если персональные данные попадут в неправильные руки, они могут быть использованы для мошенничества, кражи личности и других преступлений.
- Безопасность финансовых данных: Важно охранять финансовые данные, такие как номера кредитных карт и банковские счета, чтобы предотвратить несанкционированный доступ и финансовые потери.
- Соблюдение законодательства: В большинстве стран существует законодательство, регулирующее сбор, хранение и использование персональных данных. Организации обязаны соблюдать эти законы, чтобы избежать правовых последствий.
- Доверие пользователей: Охрана персональных данных способствует построению доверия пользователей к организациям. Если пользователи видят, что их данные хранятся и используются безопасно, они склонны доверять этим организациям.
- Поддержание репутации: Утечка персональных данных может серьезно навредить репутации организации. В случае нарушения конфиденциальности, люди могут потерять доверие к компании.
- Ограничение доступа: Охрана данных помогает ограничивать доступ к конфиденциальной информации только тем лицам, которым это действительно необходимо для выполнения своих обязанностей.
- Соблюдение этики: Охрана персональных данных является этическим обязательством, позволяющим уважать личные пространства и права людей.

GDPR - General Data Protection Regulation

Безопасность данных напрямую связана с законодательством. Существуют нормативы, регулирующие обработку и хранение данных, такие как GDPR, HIPAA, CCPA и др., в зависимости от местоположения и характера деятельности.

 **GDPR (Общий регламент защиты персональных данных) - постановление Евросоюза, усиливающее защиту персональных данных граждан ЕС.**

Усиливающее, так как многие страны ЕС уже имеют локальные законы, регулирующие защиту данных и GDPR - более “строгая” версия.

Основная цель этого постановления - дать гражданам легальную возможность управлять, передавать, корректировать и удалять свои персональные данные, хранящиеся у третьих лиц, например, в интернет-магазинах или социальных сетях.

Различные статьи GDPR позволяют гражданам следующее:

- Право на доступ — у каждого человека есть возможность получить свои данные или доступ к ним. Речь идет не только о той информации, которую он сам предоставил, но и о той, которую компания собрала о нем из других источников или даже создала сама.
- Право на уточнение — пользователь вправе потребовать корректировку информации, которая утратила достоверность или неточна, но все еще обрабатывается компанией.
- Право на удаление данных — также известное как право быть забытым. Субъект вправе потребовать от компании-контроллера удалить его данные. Например, вы можете потребовать от интернет-магазина или социальной сети удалить ваши данные.

Есть и другие права, как, например, право на ограничение обрабокти, право на переносимость данных или прав не быть объектом автоматизированного принятия решений.

В контексте дата-аналитики нужно понимать возможные ограничения на анализ данных, если они содержат даже и анонимизированные данные пользователей, которые потребовали исключить их использования при автоматизированном принятии решений. Например, пытаясь проанализировать часто заказываемые товары в магазине, вы не имеете права использовать данные клиентов, которые потребовали удаление своего аккаунта из вашей системы со всеми транзакциями. Обычно крупные организации, работающие с большим количеством персональных

данных, внедряют процессы по обработке данных пользователей и проходят специальные аудит на соответствие этих процессов GDPR.

Ключевые принципы GDPR:

1. Законность, справедливость и прозрачность — должны быть легальные основания в рамках GDPR для сбора и использования данных, соблюдение любых законов, открытость, честность от начала и до конца об использовании персональных данных.

   Веб-магазин, требующий указать пол клиента при регистрации скорее всего нарушает этот принцип GDPR, так как эта информация не нужна для осуществления бизнеса - продажи товаров.

2. Ограничение целью — обработка должна сводиться к тому, что было заявлено субъекту данных. Все конкретные задачи должны быть закреплены в политике конфиденциальности и должны четко соблюдаться.

   Если сайт знакомств декларирует, что собирает предпочтения пользователей для поиска наиболее подходящего партнера, а на самом деле использует эту информацию для показа контекстной рекламы, то этот принцип нарушается.

3. Минимизация данных — использование минимально необходимого объема данных для выполнения поставленных целей; Если данные не используются для обслуживания клиентов и различной отчетности (финансовой, аудиторской и так далее), то их нужно удалять.

   Есть ограничения на хранения данных неактивных пользователей.

4. Точность — персональные данные должны быть точными и не должны вводить в заблуждение; ошибочные данные подлежат корректировке.

5. Ограничение хранения данных — не хранить данные дольше, чем нужно, периодически проводить аудит данных и удалять неиспользуемые.

   Есть законы, требующие хранение истории заказов не менее 10 лет. Компания является GDPR-compliant, если не удаляет эти данные, хотя фактически они могут и не использоваться.

6. Целостность и конфиденциальность/безопасность — хранить данные в безопасном месте и уделять достаточное внимание сохранности данных.

7. Подотчетность — ответственность за обработку персональных данных и выполнение всех остальных принципов GDPR, включая записи о конфиденциальности, защите, использовании, проверке данных; назначении должностного лица по защите данных. Для европейской компании быть GDPR-compliant - дорогое удовольствие (нужен дополнительный персонал по защите данных и проведения аудитов).

За невыполнение закона накладывается штраф до 20 000 000 евро или до 4 % от годового мирового оборота компании за предыдущий финансовый год, в зависимости от того, что больше.

Задание для закрепления

Какие из данных достаточно собрать для корректной работы сайта по доставке пиццы?

- Имя
- Информация о работе
- Фамилия
- Медицинская информация
- Адрес электронной почты
- Фотография клиента
- Номер телефона
- Адрес проживания
- Логин и пароль
- Дата рождения
- Платежные данные
- Вкусовые предпочтения
- Информация о местоположении
- Социальные профили

Методы обеспечения безопасности данных

Основные методы, которые используются для защиты персональных данных:

- Шифрование данных: Шифрование представляет собой процесс преобразования данных в непонятный для посторонних вид. Только тот, у кого есть соответствующий ключ, может расшифровать данные и получить к ним доступ. Шифрование применяется при передаче данных через интернет, а также при хранении информации на устройствах.
- Аутентификация и авторизация: Для доступа к конфиденциальным данным используются методы аутентификации (проверка личности пользователя) и авторизации (разрешение доступа на основе прав). Включение двухфакторной аутентификации (2FA) повышает уровень безопасности, требуя наличие двух разных методов подтверждения личности.
- Обновления и патчи: Постоянное обновление программного обеспечения и операционных систем является важным методом обеспечения безопасности. Производители регулярно выпускают патчи, исправляющие уязвимости и ошибки, которые могут быть использованы злоумышленниками.
- Файрволы и антивирусные программы: Использование файрволов (программ для контроля входящего и исходящего сетевого трафика) и антивирусных программ помогает предотвратить атаки, вредоносное программное обеспечение и вирусы.
- Сегрегация данных: Разделение данных на уровни доступа, где каждый пользователь имеет доступ только к необходимой ему информации, минимизирует риск утечки данных.
- Обучение пользователей: Обучение сотрудников и пользователей соблюдению секретности и осторожности в обращении с данными также важно для предотвращения утечек и атак со стороны пользователей.
- Аудит безопасности: Ведение журналов (логов) активности пользователей и системы позволяет выявить подозрительные действия и атаки, а также отслеживать изменения и действия в системе.
- Физическая безопасность: Защита физического доступа к серверам, компьютерам и другим устройствам, на которых хранятся данные, также является ключевым аспектом обеспечения безопасности.
- Регулярная оценка уязвимостей: Проведение аудитов и тестирования на уязвимости позволяет выявить слабые места в системе и принять меры для их устранения.

Аутентификация двух факторов (2FA) - это метод обеспечения безопасности, который требует от пользователя предоставить два различных способа подтверждения своей личности перед доступом к учетной записи или системе.

Эти способы могут включать в себя что-то, что пользователь знает (например, пароль) и что-то, что пользователь имеет (например, устройство для генерации одноразовых кодов).

2FA улучшает безопасность, так как даже если злоумышленник узнает пароль, ему также понадобится доступ к другому фактору аутентификации. Это делает процесс взлома гораздо сложнее.

Факторы аутентификации включают:

- Что-то, что вы знаете: Пароль, PIN-код или ответ на секретный вопрос.
- Что-то, что вы имеете: Смартфон, устройство для генерации одноразовых кодов (например, аутентификаторы) или физический ключ.
- Что-то, чем вы являетесь: Биометрические данные, такие как скан отпечатка пальца, распознавание лица или голоса.

Комбинация двух или более факторов значительно повышает уровень безопасности и защищает аккаунты и данные от несанкционированного доступа.

Задание для закрепления

Проанализируйте следующие пароли, как думаете, какие из них более надежные и почему?

"123456"
"P@ssw0rd"
"MyDog'sName123"
"Qwerty12345"
"$ecureP@$$w0rd"

"Фишинг" (phishing) в контексте безопасности данных означает метод атаки, при котором злоумышленники пытаются обмануть пользователей с целью получения их конфиденциальных данных, таких как пароли, номера кредитных карт, персональные и финансовые сведения.

Фишинг-атаки обычно включают в себя создание ложных коммуникаций, которые кажутся быть от легитимных источников, таких как банки, онлайн-платежные системы, социальные сети или другие сервисы.

Фишинг-атаки могут принимать разные формы:

- Электронная почта: Злоумышленники отправляют электронные письма, которые выглядят так, будто они от официальных и доверенных организаций, и просит пользователя предоставить свои личные данные или перейти по ссылке на поддельный сайт.
- Сайты-подделки: Злоумышленники создают веб-сайты, которые максимально похожи на официальные сайты известных компаний или организаций. Пользователи могут случайно предоставить свои данные на таких сайтах.
- Социальные сети: Злоумышленники могут создавать ложные профили в социальных сетях, притворяться знакомыми и запрашивать личные данные или деньги.
- СМС и мессенджеры: Атаки через мобильные сообщения могут включать в себя просьбу перейти по определенной ссылке или отправить конфиденциальные данные в ответ на запрос.

Для защиты от фишинга важно быть бдительным и предостерегать подозрительные запросы на предоставление личной информации. Важно проверять адреса веб-сайтов, сравнивать их с официальными источниками, не переходить по ссылкам из электронных писем, а также использовать механизмы двухфакторной аутентификации (2FA) для дополнительной защиты учетных записей.

"Бэкап" данных - это процесс создания резервных копий информации, хранящейся на устройствах, с целью обеспечения ее сохранности и восстановления в случае потери, повреждения или катастрофы.

Бэкапы позволяют создать копии данных, которые можно использовать в случае непредвиденных событий, таких как сбои в системе, атаки вирусов, случайное удаление файлов или даже физическое повреждение устройства.

Важность бэкапов для безопасности данных обусловлена несколькими факторами:

- Предотвращение потери данных: В случае сбоев, хакерских атак, вирусов, случайного удаления или других непредвиденных ситуаций, бэкапы позволяют восстановить утраченные данные.
- Защита от катастроф: Пожары, наводнения, кражи или другие физические катастрофы могут повредить или уничтожить компьютеры и хранилища данных. Бэкапы позволяют восстановить информацию после таких событий.
- Обеспечение непрерывности бизнеса: Для организаций важно иметь доступ к важной информации даже при возникновении проблем. Бэкапы позволяют быстро восстановить работоспособность систем и продолжить бизнес-процессы.
- Защита от угроз: В случае атаки вирусами, шифровальщиками или другими злонамеренными программами, можно вернуться к бэкапам, созданным до атаки.

Для обеспечения безопасности данных рекомендуется регулярно создавать бэкапы на внешние носители, в облачные хранилища или на отдельные серверы. Важно также проверять и восстанавливать бэкапы, чтобы убедиться в их целостности и работоспособности.

Задание для закрепления

Как вы думаете, какой из перечисленных способов НЕ является хорошей практикой для создания паролей?

1. Использование длинных фраз известных стихотворений.
2. Использование комбинации больших и маленьких букв, цифр и специальных символов.
3. Использование личных данных, таких как дата рождения или имя.
4. Создание уникальных паролей для каждого аккаунта.

Что такое аутентификация двух факторов (2FA)?

1. Особый вид шифрования.
2. Система проверки двух разных паролей.
3. Метод обеспечения безопасности, который требует от пользователя предоставить два различных способа подтверждения своей личности перед доступом к учетной записи.
4. Процесс создания резервной копии данных.

Что означает термин "фишинг" (phishing) в контексте безопасности данных?

1. Процесс удаления вредоносных программ.
2. Попытка получения конфиденциальных данных путем маскировки под доверенные источники.
3. Охрана данных с помощью пароля.
4. Процесс создания копий данных.

Что такое "бэкап" данных и почему он важен для безопасности?

1. Способ взлома защиты данных.
2. Создание копии данных с целью их восстановления в случае потери, повреждения или взлома.
3. Взлом зашифрованных данных.
4. Отправка данных на удаленный сервер.