Международные требования и нормы законодательства КР: Использование спроектированной защиты данных и конфиденциальности по умолчанию (privacy by design и privacy by default) в процессе разработки информационных систем и формирования системы кибербезопасности

Тимур Талгатович Губаев

Независимый эксперт, офицер по кибербезопасности, специалист медико-информационных систем

Использование спроектированной защиты данных и конфиденциальности по умолчанию (Privacy by Design и Privacy by Default) в процессе разработки информационных систем и формирования системы кибербезопасности"

Тимур Губаев

Бишкек 2023

Спроектированная защита данных (конфиденциальность по дизайну)

- Спроектированная защита данных - это принцип, который гласит, что конфиденциальность должна быть встроена в организационные процессы, архитектуру и разработку продукта или услуги с самого начала.
- Будущее конфиденциальности ПДн не может быть обеспечено исключительно соблюдением нормативных рамок
- В своей работе организации должны учитывать потерю конфиденциальности на каждом этапе процесса разработки, от проектирования до реализации, тестирования и обслуживания.
- Спроектированная защита данных может помочь предотвратить нарушения конфиденциальности и неправильное использование данных.

Важность принципа спроектированной защиты данных при разработке информационных систем

- Принцип помогает обеспечить защиту личной информации и данных пользователей на протяжении всего жизненного цикла системы.
- Помогает предотвратить нарушения конфиденциальности и неправильное использование данных.
- Кроме того, конфиденциальность может помочь построить доверие между пользователями и организациями, поскольку пользователи будут знать, что их личная информация защищена на каждом этапе процесса разработки.

Примеры спроектированной защиты данных на практике

Существует множество организаций, которые внедрили спроектированную защиту данных в свои продукты и услуги, например:

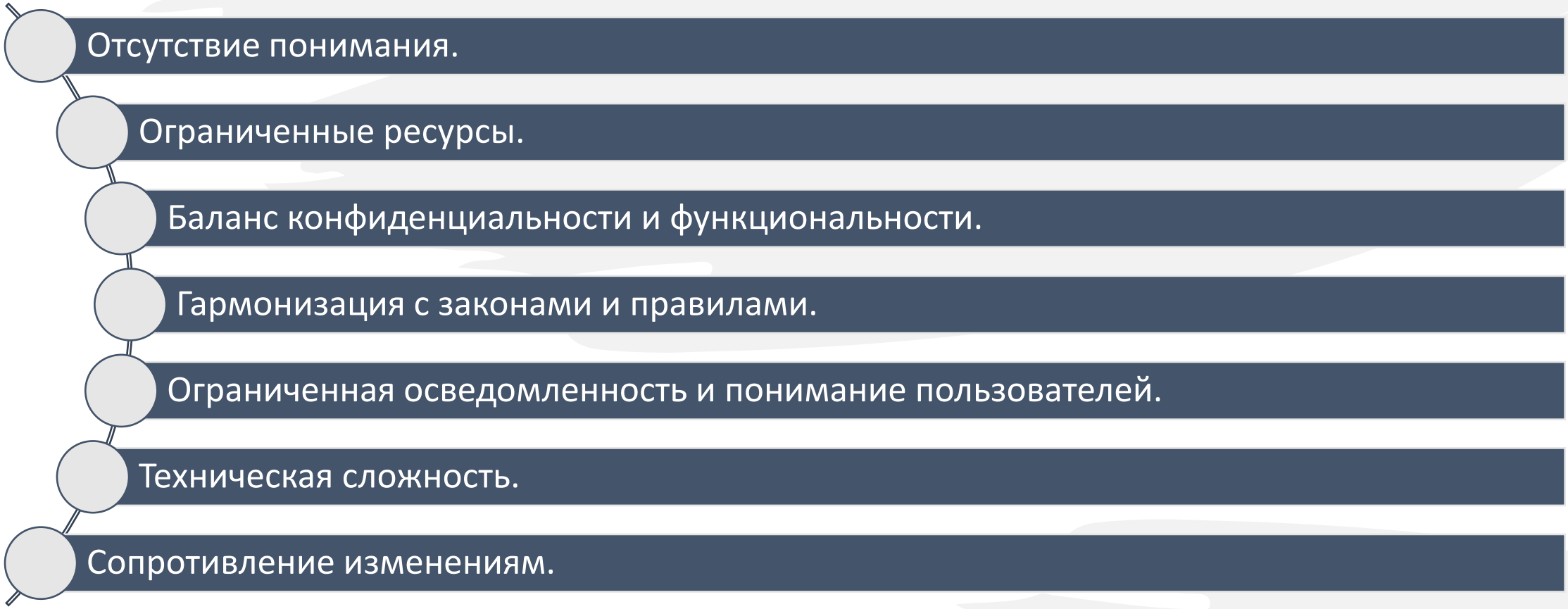
- Google: внедрил принципы в свои продукты и услуги, встроив конфиденциальность в свой процесс разработки
- Microsoft: один из первых внедрил принципы в свои продукты и службы, включив соображения конфиденциальности в свой процесс разработки
- Apple: внедрил принципы конфиденциальности по дизайну в свои продукты и услуги, уделяя большое внимание конфиденциальности пользователей

У этих компаний есть специальная команда по обеспечению конфиденциальности, которая работает над тем, чтобы обеспечить защиту пользовательских данных на протяжении всего жизненного цикла продукта и услуг.

Конкретные методы конфиденциальности по дизайну

- Минимизация данных: ограничение сбора, использования и хранения личной информации тем, что строго необходимо для достижения цели продукта или услуги.
- Шифрование: преобразование личной информации в такой вид, чтобы она не могла быть прочитана неавторизованными лицами.
- Контроль доступа: ограничение доступа к личной информации только теми, кто в ней нуждается.
- Оценка воздействия на конфиденциальность: оценка потенциальных рисков конфиденциальности продукта или услуги и определение способов снижения этих рисков.
- Элементы управления конфиденциальностью, ориентированные на пользователя: предоставление пользователям возможности управлять своими настройками конфиденциальности.

Проблемы реализации конфиденциальности по дизайну



Понимая эти проблемы, компании могут быть лучше подготовлены к их преодолению и успешно внедрять конфиденциальность по дизайну в свои продукты и услуги

Способы преодоления проблем реализации спроектированной защиты данных

- Отсутствие понимания: инвестиции в обучение своих сотрудников, чтобы помочь им понять, что такое конфиденциальность по дизайну и как ее реализовать.
- Ограниченные ресурсы: приоритетное внимание стоит уделить реализации конфиденциальности по дизайну в наиболее важных областях своих продуктов или услуг.
- Баланс конфиденциальности и функциональности: возможно вовлечение пользователей в процесс проектирования, чтобы гарантировать, что элементы управления конфиденциальностью интегрированы таким образом, чтобы это не оказывало негативного влияния на функциональность продукта или услуги.
- Гармонизация с законами и правилами: построение процессов для регулярного пересмотра и обновления своих политик и процедур конфиденциальности для обеспечения соответствия действующим законам и правилам.
- Ограниченная осведомленность и понимание пользователей: предоставление пользователям тренингов, как использовать элементы управления конфиденциальностью
- Техническая сложность: возможен найм экспертов по конфиденциальности или специализированных компаний с необходимым опытом, чтобы помочь им реализовать конфиденциальность по дизайну.
- Сопротивление изменениям: важно донести преимущества конфиденциальности по дизайну до ключевых заинтересованных сторон и вовлечь их в процесс проектирования.
- Интеграция с существующими системами: проведение тщательной оценки своих существующих систем для выявления потенциальных проблем совместимости.

Стоит отметить, что некоторые из этих проблем тесно связаны, и реализация одного решения может повлиять на другие проблемы. Важно иметь комплексный подход и понимать, что реализация конфиденциальности по дизайну является непрерывным процессом, который требует постоянного мониторинга и улучшения.

Конфиденциальность по умолчанию

Конфиденциальность по умолчанию — это принцип, который гласит, что настройки конфиденциальности должны быть установлены на самый высокий уровень защиты по умолчанию и используется принцип спроектированной защиты данных по всему жизненному циклу процессов и ПО

Принцип требует, чтобы защита персональных данных была включена по умолчанию для всех систем и услуг организации: все процессы, жизненный цикл систем, архитектура, принцип обработки и хранения ПДн.

Организации должны разрабатывать свои продукты и услуги с учетом конфиденциальности с самого начала, а не добавлять функции конфиденциальности в по остаточному методу.

Важность принципа конфиденциальности по умолчанию при разработке информационных систем

Конфиденциальность по умолчанию важна при разработке информационных систем, поскольку она помогает защитить личную информацию и данные пользователей от сбора и использования без их согласия.

Это также помогает предотвратить использование компаниями данных пользователей для собственной выгоды.

Принцип может помочь укрепить доверие между пользователями и компаниями, поскольку пользователи будут знать, что их личная информация защищена с самого начала.

Примеры конфиденциальности по умолчанию на практике

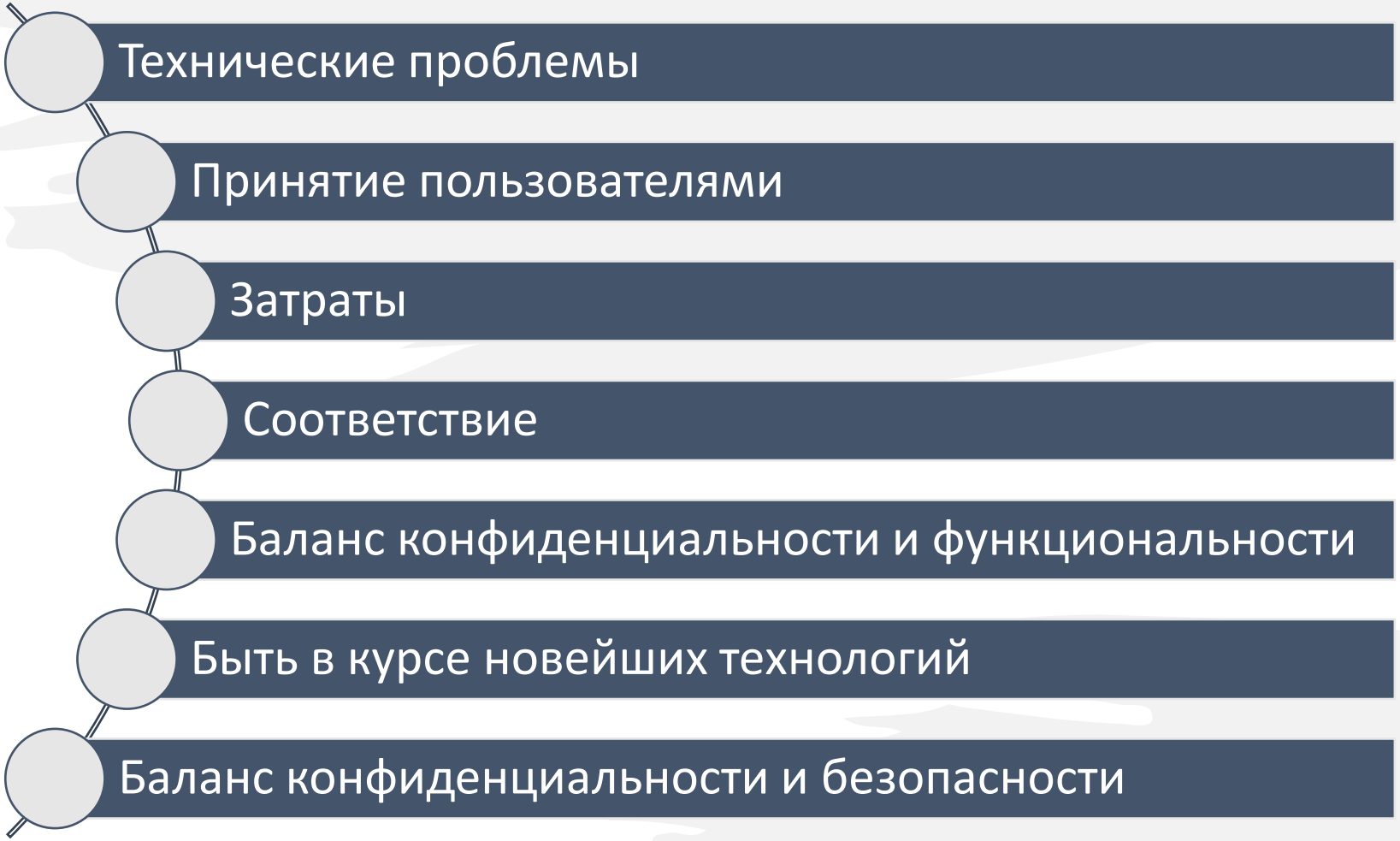
Существует множество организаций, которые внедрили конфиденциальность по умолчанию в свои продукты и услуги, например:

- Google: продукты Chrome, Android и Gmail. Функционал: режим инконгито с удалением данных браузера, автоматическое удаление хранимых браузером данных
- Microsoft: продукты Windows, Edge. Функционал: Windows Hello с защитой доступа к учётной записи на ПК, предотвращение отслеживание с блокировкой отслеживающих файлов
- Apple: продукты iOS, Safari. Функционал: ограничение отслеживания рекламой для отказа от показа целевой рекламы, вход с Apple для входа в приложения и сайты без обмена личной информацией.
- Mozilla: продукт Firefox. Функционал: блокировка сторонних файлов cookie, блокировка трекеров и скриптов
- Signal: продукт Signal. Фунцкционал: шифрование от начала до конца (end-to-end) и принцип отсутствия сбора данных о пользователях
- DuckDuckGo: продукт DuckDuckGo Search. Функционал: принцип отсутствия отслеживания поисковых запросов, блокировка сторонних трекеров и уровень конфиденциальности с показом уровня защиты веб-сайта

Конкретные методы конфиденциальности по умолчанию

- Ограниченный сбор данных: Одним из ключевых методов обеспечения конфиденциальности по умолчанию является ограничение объема собираемых персональных данных.
- Удобные для конфиденциальности значения по умолчанию: настройка системы на то, чтобы по умолчанию были включены наиболее безопасные настройки конфиденциальности.
- Механизмы согласия: пользователи активно дают свое согласие на сбор, использование и передачу своих персональных данных.
- Шифрование и анонимизация: шифрование и анонимизация персональных данных может помочь защитить их от несанкционированного доступа и раскрытия.
- Регулярный мониторинг и тестирование: непрерывный мониторинг за средствами защиты и событиями, регулярное тестирование на проникновение, аудит безопасности и оценку воздействия на конфиденциальность.

Проблемы реализации конфиденциальности по умолчанию



Способы преодоления проблем реализации конфиденциальности по умолчанию

- **Техническая реализация, Затраты**: внедрение шаг-за-шагом, то есть начало в небольшой, управляемой части своего продукта или услуги с дальнейшим расширением внедрения.
- **Принятие пользователями**: информирование пользователей о преимуществах конфиденциальности по умолчанию и о том, как она защищает их личные данные.
- **Соответствие**: обратиться за юридическими и нормативными указаниями к юридическим компаниям для обеспечения того, чтобы их продукты или услуги соответствовали соответствующим законам и правилам конфиденциальности.
- **Техническая реализация, Недостаточная осведомленность и понимание**: привлечение экспертов по конфиденциальности.
- **Быть в курсе новейших технологий**: постоянный мониторинг и совершенствование, таким образом необходимо постоянно отслеживать новейшие технологии и лучшие практики.
- **Баланс конфиденциальности и безопасности, Баланс конфиденциальности и функциональности**: возможно использовать спроектированную защиту в качестве основы для создания конфиденциальности на каждом этапе процесса разработки.
- **Создание культуры конфиденциальности**: организации должны создать культуру конфиденциальности у себя внутри

Принципы в жизненном цикле разработки программного обеспечения (SDLC)

Жизненный цикл разработки программного обеспечения (SDLC) — это процесс, в котором описываются этапы, связанные с разработкой программного обеспечения. Обычно он включает в себя следующие этапы:

- Сбор требований: На этом этапе проектная группа работает над пониманием потребностей и целей программного обеспечения.
- Проектирование: на этом этапе команда создает высокоуровневый дизайн программного обеспечения, включая общую архитектуру, модель данных и пользовательский интерфейс.
- Реализация: На этом этапе команда начинает писать код и строить программное обеспечение в соответствии с дизайном.
- Тестирование: на этом этапе команда тестирует программное обеспечение, чтобы убедиться, что оно соответствует требованиям и функциям, как и предполагалось.
- Развертывание: на этом этапе программное обеспечение развертывается в рабочей среде, где оно становится доступным для пользователей.
- Обслуживание: На этом этапе программное обеспечение поддерживается и обновляется для решения любых проблем или изменений, которые могут возникнуть.

Для чего нужно использовать SDLC совместно с принципами?

Чтобы гарантировать, что разрабатываемое программное обеспечение соответствует стандартам конфиденциальности и безопасности.
Например:

- на этапе сбора требований команда может определить, какие данные являются конфиденциальными и какие меры необходимо реализовать для их защиты.
- на этапе проектирования команда может реализовать методы минимизации данных и защиты данных, такие как шифрование и контроль доступа.
- на этапе тестирования команда может протестировать систему, чтобы убедиться, что она соответствует требованиям конфиденциальности и безопасности.

И всё-таки, как реализовать принципы конфиденциальности по дизайну и конфиденциальности по умолчанию в организации 1/2

- Включение соображений конфиденциальности в фазу сбора требований.
- Проведение оценки воздействия на конфиденциальность (PIA):
  это инструмент, который помогает выявлять и оценивать потенциальные риски конфиденциальности проекта.
- Реализация политик минимизации и хранения данных.
- Предоставление пользователям четкой и прозрачной информации:
  предоставление политики конфиденциальности, которая легко доступна и понятна.
- Внедрение механизмов согласия, а не отказа:
  если пользователь не дал согласия, это не значит, что организации разрешено работать с его ПДн.
- Реализация детальных элементов управления:
  возможность контролировать типы данных, собираемых и используемых, а также контролировать частоту сбора.

Реализация принципов конфиденциальности по дизайну и конфиденциальности по умолчанию в организации 2/2

- Тестирование и мониторинг средств защиты конфиденциальности:
  регулярное тестирование и мониторинг системы для выявления и устранения любых рисков конфиденциальности.
- Постоянный мониторинг и совершенствование:
  быть в курсе последних технологий и лучших практик.
- Привлечение экспертов по конфиденциальности: найм сотрудника по конфиденциальности, привлечение консультанта по конфиденциальности или привлечение эксперта по конфиденциальности в команду разработчиков.
- Обучение сотрудников: обучение правилам защиты данных и передовым практикам, а также тому, как выявлять и устранять риски конфиденциальности.
- Будьте в курсе меняющихся правил защиты данных:
  отслеживание последних рекомендаций и передовой практики регулирующих органов.
- Реализация дружественных к конфиденциальности настроек: ограничение сбора и обмена персональными данными, а также предоставление пользователям четкой и прозрачной информации об использовании данных.

Преимущества внедрения принципов

- Повышение доверия: демонстрируя приверженность защите личной информации, организации могут построить доверие со своими пользователями и клиентами.
- Снижение риска утечек данных: уже на этапе внедрения принципов, организации могут снизить риск утечек данных и защитить личную информацию.
- Соблюдение законов и правил: внедрив принципы, организации могут гарантировать, что они соответствуют законам и правилам, касающимся личной информации.
- Репутационное преимущество: организации могут выделить себя на фоне других организаций, подчеркивая защиту личной информации.
- Улучшенный пользовательский опыт: предоставляя управление конфиденциальностью, ориентированные на пользователя, организации могут дать им возможность принимать решения о своей личной информации и улучшать общий пользовательский опыт.

Заключение

Реализуя принципы, организации могут помочь защитить личную информацию пользователей и завоевать доверие своих пользователей. Кроме того, это поможет соблюдать последние правила конфиденциальности и безопасности.

Внедряя принципы конфиденциальности по дизайну, эти компании и организации могут предоставлять своим пользователям продукты и услуги, которые являются функциональными и безопасными, и помогают построить доверие со своими пользователями, демонстрируя свою приверженность защите личной информации