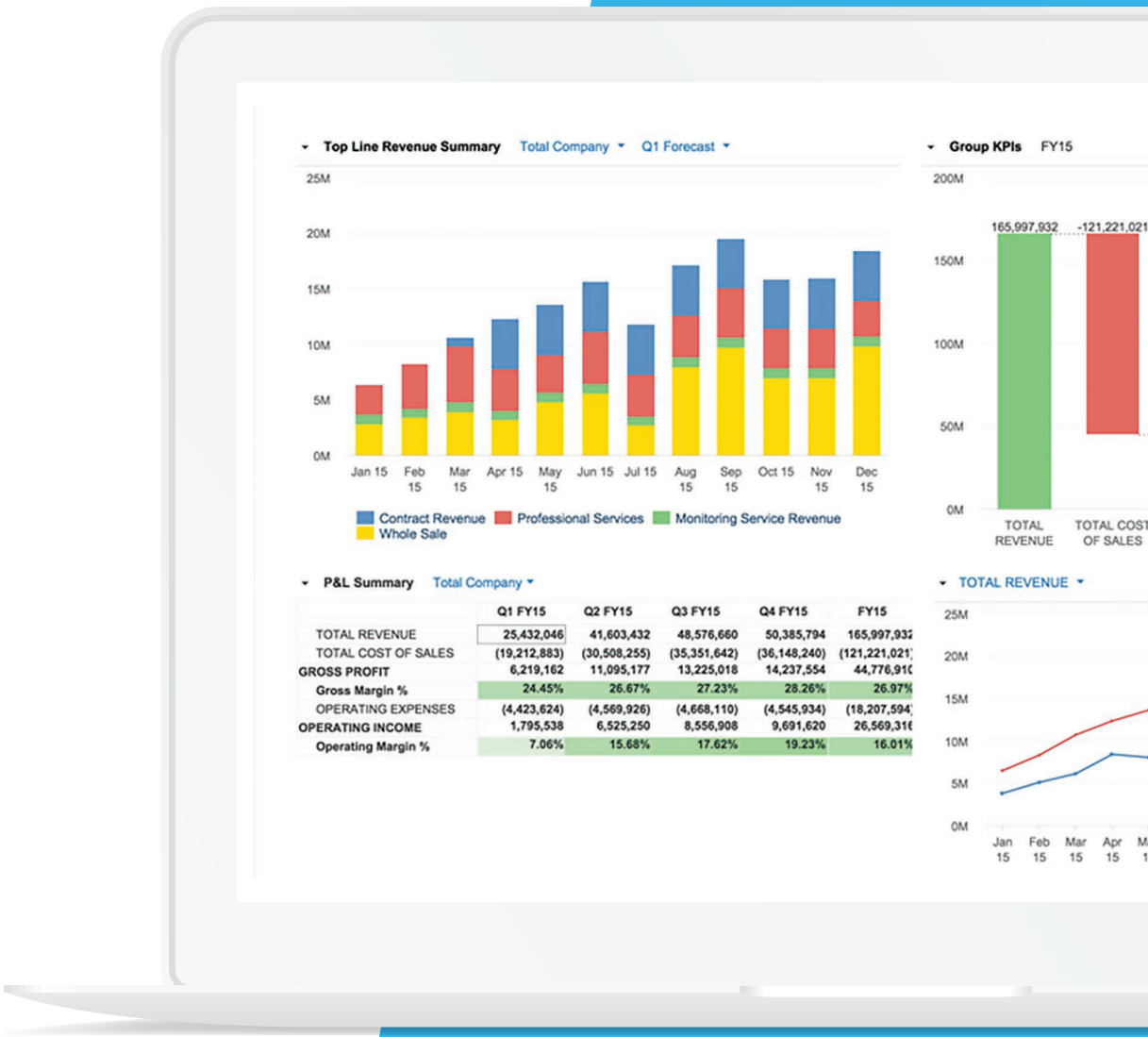
anaplan ТЕХНИЧЕСКАЯ ДОКУМЕНТАЦИЯ

Обзор принципов безопасности



ОСНОВНЫЕ ЦЕЛИ

Безопасность данных для нас всегда стоит на первом месте. Платформа Anaplan была создана на основе ключевых принципов обеспечения информационной безопасности, также известных как модель CIA.

Конфиденциальность (confidentiality) — информация может быть раскрыта только уполномоченым лицам или системам.

Целостность (integrity) — контроль и обеспечение точности и согласованности данных на протяжении всего жизненного цикла.

Доступность (availability) — гарантия доступности информации при необходимости.

Anaplan ответственно придерживается этих принципов, поскольку на кону стоит доверие наших клиентов. Неотъемлемой частью работы Anaplan является обеспечение надежной системы безопасности и программ защиты конфиденциальной информации, включая информацию, предоставляемую клиентами для наших служб («данные клиентов»).

О компании

С момента основания Anaplan мы стремимся соответствовать этим принципам, обеспечивая надежную защиту информационных систем от угроз безопасности, а также их быстрое аварийное восстановление. Все функциональные отделы компании находятся в разных странах мира, что снижает риски, связанные с локальными событиями в том или ином регионе.

Офисы в США в основном отвечают за продажи, маркетинг и техническую поддержку. Сотрудники офисов в Великобритании и Сингапуре обеспечивают региональное присутствие, а также оказывают поддержку в сфере резервного копирования данных.

В Великобритании сотрудники занимаются разработкой основных продуктов при поддержке своих коллег из США, Франции и России. Исходные коды хранятся в отдельном центре обработки данных. Все работники, которые занимаются разработкой, тестированием и технической поддержкой, могут работать удаленно благодаря безопасному VPN-соединению с двухфакторной авторизацией и обеспечивать бесперебойную разработку и техническую поддержку в случае нарушения работы главных офисов.

Anaplan внедряет ряд процессов, которые гарантируют быстрое и эффективное восстановление работы служб в случае серьезных сбоев согласно плану работ в аварийных ситуациях.

Локальное и удаленное резервное копирование данных, возможность быстрого восстановления и запас мощности инфраструктуры, доступность вспомогательных центров обработки данных, географически разрозненная структура компании и персонал службы поддержки гарантируют быстрое и эффективное восстановление служб после серьезного сбоя согласно планам работ при аварийных ситуациях.

Архитектура

Оборудование Anaplan размещено на сторонних объектах (в «центрах обработки данных»). За исключением систем обеспечения, таких как энергообеспечение, освещение, противопожарная система и т. д., инфраструктура центров обработки данных полностью принадлежит компании Anaplan, которая осуществляет контроль, управление и поддержку этих центров.

ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ

- Центры обработки данных Anaplan расположены в штате Вирджиния (США) и в Амстердаме (ЕС). Их расположение было выбрано с учетом низкой вероятности землетрясений, наводнений и других крупных стихийных бедствий.
- Предварительно каждый объект прошел строгую проверку на наличие, внедрение и соблюдение мер физической безопасности.
- Каждый объект круглосуточно без выходных охраняется сотрудниками службы охраны, ограждением с высокой степенью безопасности, также работает система видеонаблюдения. Доступ и действия на объекте заносятся в журнал, записываются на видео и хранятся в течение не менее 30 дней.
- Для входа на каждый объект требуется предварительная авторизация, паспортный контроль и подтверждение биометрических данных.
- Объекты ежегодно проверяются ведущими в отрасли компаниями на соблюдение стандартов ISO 27001 и/или SSAE 16 тип II. Anaplan регулярно проводит проверки своих центров обработки данных.
- Компания пользуется услугами таких поставщиков технологий, как Cisco, Dell, EMC, F5, HP и RSA.

В Anaplan используются приведенные ниже стандарты обеспечения безопасности и конфиденциальности, проверок и сертификации.

- ISO 27002:2013: Anaplan взяла за основу своей политики информационной безопасности стандарты ISO 27000. Компания разработала и внедрила этот стандарт для соблюдения бизнес-требований.
- Отчеты SOC: среда управления безопасностью в центрах обработки данных Anaplan проходит проверку по форме отчета SSAE 16 (SOC-1). Центр обработки данных в ЕС также имеет сертификат ISO 27001. Anaplan начала проводить проверки SOC с середины 2015 г.
- Самостоятельная сертификация Safe Harbor: в отношении информации, предоставляемой клиентами, Anaplan проводит самостоятельную сертификацию на соответствие принципам соглашений Safe Harbor между ЕС и США и Швейцарией и США, которые были инициированы Министерством торговли США.
- Знак конфиденциальности TRUSTe Privacy Seal: Anaplan получила знак конфиденциальности TRUSTe Privacy Seal, подтверждающий, что положение о конфиденциальности на веб-сайте Anaplan было проверено TRUSTe на соответствие требованиям программы TRUSTe, включая прозрачность, надежность и возможность выбора в отношении сбора и использования персональных данных.
- Знак TRUSTe Safe Harbor: Anaplan получила знак TRUSTe EU Safe Harbor и придерживается стандартов EU Safe Harbor Framework, установленных Министерством торговли США и Европейским союзом в отношении Anaplan.

ИНФРАСТРУКТУРА РЕЗЕРВИРОВАНИЯ

Инфраструктура Anaplan имеет резервный «активный/пассивный» дизайн для обеспечения непрерывной работы в случае сбоя. Ни один сбой какого-либо компонента не должен приводить к сбою клиентской службы и потере данных, предоставленных клиентами. В случае первичного сбоя архитектура резервирования обеспечит непрерывность работы за счет задействования вспомогательных систем.

ИНФРАСТРУКТУРА БЕЗОПАСНОСТИ

Защита каждого объекта осуществляется с помощью системы безопасности с многоуровневой архитектурой, состоящей из брандмауэров, систем обнаружения вторжений (IDS), антивирусных/антишпионских программ, и возможностью мониторинга.

ИНФРАСТРУКТУРА СЕТИ

Инфраструктура внутренней сети разделена на надежные сегменты с помощью брандмауэров, виртуальных сетей (VLAN) и списков контроля доступа (ACL), которые ограничивают доступ и коммуникацию между системами. Ни одна система и ни одно лицо не может получить доступ к другой системе без получения соответствующей авторизации.

ИНФРАСТРУКТУРА СЕРВЕРА

- Все серверы работают под управлением ОС Linux® и защищены согласно политике на основе стандартов Center for Internet Security (CIS).
- Все узлы подлежат регулярной проверке, обновлению и обслуживанию.
- Все узлы периодически сканируются на наличие уязвимостей и угроз безопасности с помощью лучшей в отрасли программы Nessus®.
- Все серверы управляются и контролируются с помощью системы автоматизации для обеспечения единообразия конфигурации во всей среде.

Управление безопасностью

При разработке Anaplan применялись высокие стандарты безопасности, начиная от сетей и серверов, до получения доступа пользователями и управления данными. Платформа Anaplan представляет собой уникальную технологию, разработанную компанией Anaplan, для безопасного сбора и хранения данных, которая при этом достаточно гибка для работы с внешними системами.

В Anaplan используется программный стек с поддержкой **ACID**, который гарантирует постоянную безопасность данных.

Атомарность требует либо полного выполнения каждой транзакции, либо ее отмены. Если происходит сбой какой-либо части транзакции, то происходит отмена всей транзакции и модель остается без изменений.

Единообразие позволяет сохранять работоспособность модели при внедрении любых изменений.

Изоляция позволяет выполнять большое количество транзакций одновременно и независимо друг от друга.

Устойчивость к внешним факторам позволяет сохранить состояние транзакции после выполнения даже в случае сбоя или ошибки.

- Основное программное обеспечение включает систему обработки данных в оперативной памяти, позволяющую максимально быстро получить результаты вычислений, при этом все изменения заносятся в журнал на жестком диске в режиме реального времени.
- Полная модель данных хранится в зашифрованной сети хранения данных (SAN).
- Перед тем как применить какие-либо изменения в памяти, журналы запросов пользователей записываются на жесткий диск.
- Хранение и доступ к данным осуществляется через единый защищенный интерфейс.
- Нешифрованные данные никогда не попадают в Интернет.
- В центрах обработки данных запрещено использовать Wi-Fi и съемные носители.

ДОСТУП ПОЛЬЗОВАТЕЛЕЙ, УПРАВЛЕНИЕ И ПОЛИТИКИ

Anaplan поддерживает широкий спектр настраиваемых способов управления безопасностью, которые обеспечивают для клиентов защиту при использовании Anaplan. Эти способы включают:

- Уникальные идентификаторы пользователей (ID пользователей) для обеспечения выполнения конкретных действий только ответственным лицом.
- Блокировку доступа после нескольких неудачных попыток входа в систему.
- Смену созданного системой пароля после первого входа.
- Смену пароля после определенного периода использования.
- Завершение сеанса работы, если пользователь неактивен в течение определенного времени.
- Пароль должен отвечать следующим требованиям:
  - » состоять минимум из 8 символов;
  - » иметь минимум один символ в верхнем регистре;
  - » иметь минимум один символ в нижнем регистре;
  - » иметь минимум одну цифру;
  - » должен меняться каждые 90 дней.

Новым пользователям по умолчанию запрещен доступ к любым данным. Доступ предоставляется администратором, назначенным клиентом.

Anaplan полностью поддерживает SAML 2.0 SSO (сервер единого входа) и может использоваться клиентами, желающими полностью контролировать своих пользователей с помощью централизованной системы управления. Использование SSO позволяет клиенту полностью контролировать процесс аутентификации пользователей. Сюда относятся правила надежности пароля, окна доступа в зависимости от времени суток, двухфакторная аутентификация и другие способы управления, требуемые правилами безопасности клиента.

ДОСТУП СОТРУДНИКОВ ANAPLAN, УПРАВЛЕНИЕ И ПОЛИТИКИ

- Доступ сотрудникам к производственной инфраструктуре предоставляется только с помощью двухфакторной аутентификации RSA через безопасное VPN-соединение.
- Доступ к любому серверу центра обработки данных дополнительно защищен обязательной технологией инфраструктуры открытых ключей (PKI) SSH.
- Сотрудники не имеют права доступа к данным клиентов.
- Все данные клиента принадлежат только ему.
- Сотрудники Anaplan не могут просматривать какие-либо данные конечного пользователя без предоставления этим клиентом разрешения с помощью исходной системы управления доступом.
- Доступ основан на принципе безопасности информации по «минимальной привилегии» с разрешением доступа строго для определенного круга специалистов.
- Каждый вход проверяется и заносится в журнал.
- Все сотрудники проходят специальную проверку анкетных данных перед приемом на работу.
- Все сотрудники проходят обучение по обеспечению безопасности документированной информации и по процедурам конфиденциальности.
- Все сотрудники подписывают «Соглашения по обеспечению конфиденциальности данных клиентов».
- Все сотрудники в отделах разработки, обеспечения качества, технической эксплуатации и безопасности проходят дополнительное обучение по вопросам безопасности.
- Все разрешения на доступ немедленно аннулируются при расторжении трудового договора.

ОТДЕЛ ПО БЕЗОПАСНОСТИ

В Anaplan ряд штатных сотрудников по всему миру отвечает за управление, риски, проверку и соответствие стандартам в области безопасности и конфиденциальности. Каждый сотрудник имеет многолетний опыт работы в отрасли и один или несколько признанных в индустрии сертификатов, в том числе CISSP, CISM, CISA, CIPT, CIPM, CIPP/US, Sec+ и Net+.

Управление уязвимостью и вредоносным ПО

ВРЕДОНОСНОЕ ПО И ВИРУСЫ

Anaplan никогда не допустит внедрения вируса или вредоносного ПО в системы клиентов. Все вложения и другие данные, предоставляемые Anaplan клиентом, тщательно проверяются на наличие вирусов и вредоносного ПО.

УПРАВЛЕНИЕ УЯЗВИМОСТЬЮ ВЕБ-ПРИЛОЖЕНИЯ

Веб-приложение Anaplan регулярно сканируется средствами WAS от ведущего в области безопасности и соответствия поставщика, компании QualysGuard®. Также сканирование выполняется с использованием технологий Nessus® и Burp Scanner®.

СКАНИРОВАНИЕ НА НАЛИЧИЕ ВРЕДОНОСНОГО ПО В ВЕБ-ПРИЛОЖЕНИИ

Веб-приложение Anaplan раз в неделю сканируется на наличие вредоносного ПО (MDS) средствами от ведущего в области безопасности и соответствия поставщика, компании QualysGuard®.

Процедуры, политики и журналы безопасности

Мониторинг всех служб осуществляется как с помощью внутренних, так и внешних систем. Для повышения безопасности работа с Anaplan осуществляется в соответствии с приведенными ниже процедурами.

ЖУРНАЛЫ БЕЗОПАСНОСТИ

- Все системы (например, брандмауэры, маршрутизаторы, коммутаторы сети и операционные системы), используемые при предоставлении Anaplan, будут заносить информацию о каждом действии в соответствующий системный журнал и на централизованный сервер syslog.
- Каждый доступ клиента или сотрудников к информации проверяется и заносится в журнал.
- Все изменения данных клиентом или сотрудниками проверяются и заносятся в журнал.
- Журналы хранятся минимум 365 дней.
- Журналы будут храниться в безопасном месте во избежание несанкционированного доступа.

Журналы проверки включают перечисленные ниже позиции.

- Дату, время и часовой пояс события.
- Использованный URL-адрес или ID объекта, выполнившего действие.
- Идентификацию системы или компонента.
- Тип события, выполненного действия (просмотр, изменение и т. д.).
- Успешность или сбой выполнения.
- ID пользователя.
- IP-адрес клиента*.

* Недоступен, если клиент или его поставщик интернет-услуг использует механизм NAT (преобразование сетевых адресов) или PAT (преобразование адресов портов).

- Ни при каких обстоятельствах не выполняется запись паролей.

Шифрование данных

Anaplan использует стандартные для отрасли способы шифрования для защиты данных клиентов и коммуникаций во время передачи информации между сетью клиента и Anaplan.

- Все данные, передаваемые между клиентом и сервером, шифруются с помощью HTTPS с использованием TLS 1.2. Обмен ключами осуществляется с помощью браузера с использованием 2048-битных сертификатов. Длина ключа сеанса определяется браузером конечного пользователя с помощью максимально надежного уровня шифрования.
- Остальные данные в системе хранятся в уникальном несчитываемом двоичном формате, а диск, на котором они находятся, полностью зашифрован по технологии AES-256.

Резервное копирование

- Все данные на объекте хранятся на резервных зашифрованных сетевых дисках сети SAN по технологии AES-256, согласно принятым в отрасли стандартам.
- Потоковая передача данных также выполняется в режиме реального времени в удаленный центр резервного копирования и аварийного восстановления данных с помощью 2048-битного шифрования SSL.
- Резервные данные хранятся в зашифрованном виде по технологии AES-256.

Кроме того:

- Изменения моделей легко можно отменить и в течение нескольких секунд вернуть к предыдущей версии.
- Конечные пользователи по желанию могут выполнять архивирование моделей на своих рабочих местах.
- Все внесенные пользователями изменения просматриваются и могут быть легко отменены.
- Хранение данных осуществляется более чем в одном месте, и каждая модель копируется на вспомогательное устройство, которое активируется в случае выхода из строя основного блока.

ПРОЦЕДУРА ВОССТАНОВЛЕНИЯ

Если требуется восстановить данные, а журнал приложения недоступен, используются резервные копии в сети хранения данных объекта. Время восстановления может отличаться в зависимости от объема данных, восстанавливаемых из SAN, однако восстановление одного сервера обычно занимает не более нескольких часов.

Восстановление после аварийного сбоя

Разработанные планы восстановления после аварийного сбоя тестируются как минимум раз в год.

- Последнее полное тестирование было выполнено в августе 2015 г.

В Anaplan для восстановления после аварийного сбоя используются те объекты, где есть необходимое оборудование, программное обеспечение и интернет-подключение, а также которые географически удалены от основных центров обработки данных. Если производственные возможности в основных центрах обработки данных становятся недоступны, будут активированы и переведены в онлайн-режим функции DR. Поскольку данные клиентов уже переданы и сохранены на таких объектах, время восстановления будет существенно сокращено.

Планы Anaplan по восстановлению после аварийного сбоя в настоящий момент направлены на выполнение следующих задач:

а) RTO (целевое время восстановления) в течение 12 часов после сообщения о сбое;

б) RPO (целевая точка восстановления) в течение 30 минут.

Обслуживание системы

Обслуживание проводится вне рабочего времени, обычно по воскресеньям с 13:00 до 17:00 по тихоокеанскому времени. Обслуживание, как правило, предшествует выпуску новой версии, обычно каждые 4–6 недель.

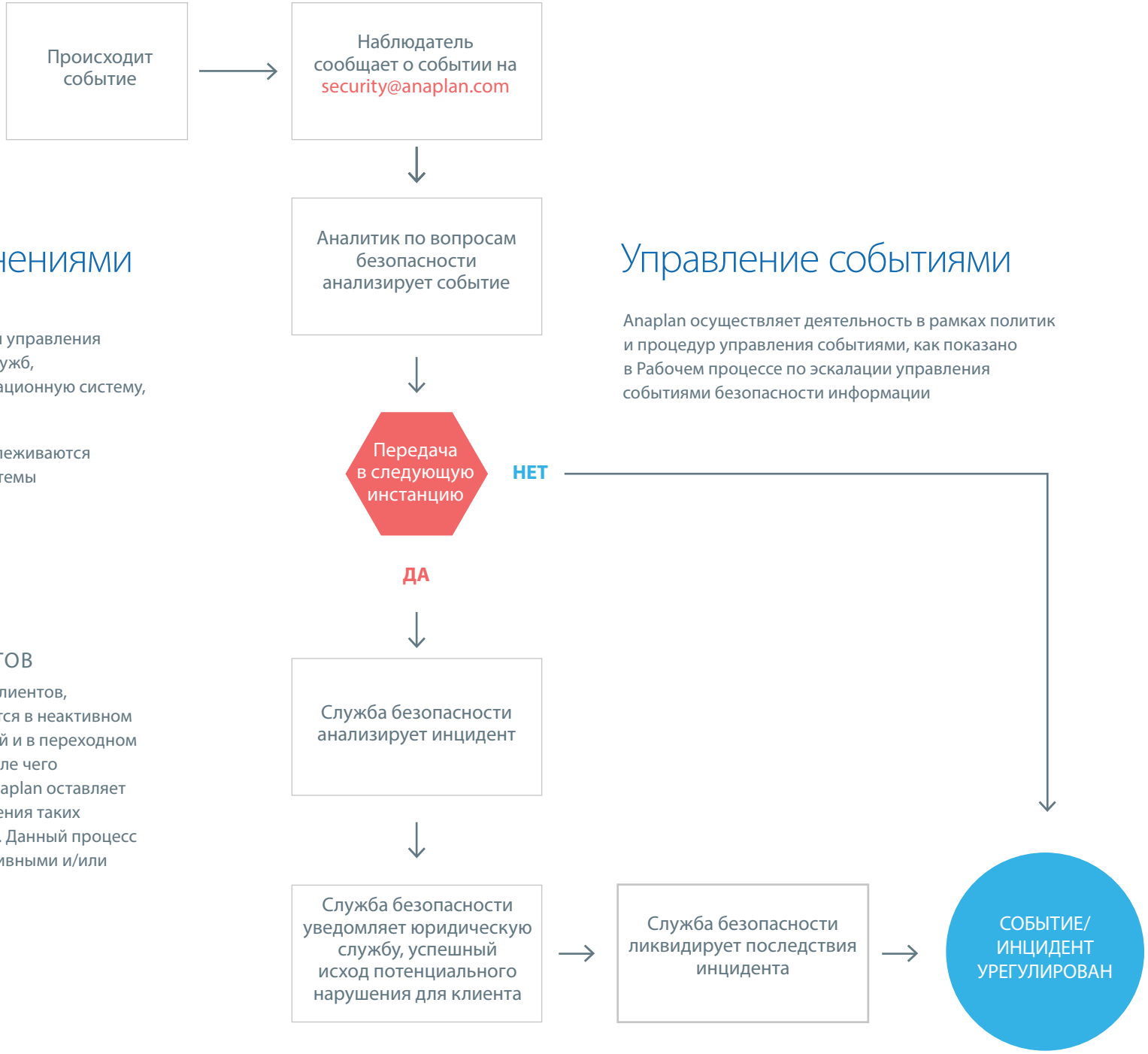
Управление изменениями

- Anaplan соблюдает полностью задокументированные процедуры управления изменениями для всех уровней служб, охватывающих приложения, операционную систему, сервер и слои сети.
- Все изменения конфигурации отслеживаются и контролируются с помощью системы отслеживания ошибок.

Данные клиентов

УДАЛЕНИЕ ДАННЫХ КЛИЕНТОВ

При расторжении договора данные клиентов, предоставленные Anaplan, сохраняются в неактивном состоянии в Anaplan в течение 30 дней и в переходном состоянии в течение еще 30 дней, после чего перезаписываются или удаляются. Anaplan оставляет за собой право уменьшить срок хранения таких данных после расторжения договора. Данный процесс регулируется действующими нормативными и/или контрактными требованиями.



Управление событиями

Anaplan осуществляет деятельность в рамках политик и процедур управления событиями, как показано в Рабочем процессе по эскалации управления событиями безопасности информации

О компании Anaplan

Anaplan — облачная платформа для корпоративного планирования, в которой объединены мощная система планирования и моделирования, возможности для совместной работы в облаке и простой интерфейс для бизнес-пользователей. Клиенты Anaplan могут выбирать более чем из 100 готовых приложений для планирования в рамках Anaplan App Hub или же легко создавать собственные приложения. Anaplan — это частная компания со штаб-квартирой в Сан-Франциско и представительствами на четырех континентах.

Больше информации на **anaplan.ru**.


company/anaplan


@anaplan


/anaplan


+anaplanInc