Введение в OLAP и современные технологии бизнес-планирования

Как компании используют данные для управления и планирования бизнеса в эпоху цифровой трансформации

10 лекций: от архитектуры OLAP до IBP, S&OP и бюджетирования

Автор курса: Сулейменов Я.
Платформа: CasPlan.tech
2025

Информационная безопасность и управление данными

- Риски Excel (утечки, дубли, ошибки)
- OLAP: разграничение прав доступа, контроль версий
- Работа с мастер-данными
- Аргументы для ИТ и CFO
- Регуляторные требования и доверие к данным

CasPlan

Кибернетика

MaxPlan Solutions

Безопасность и доверие к данным: основа IBP

Техническая безопасность

Триада CIA: основа технической безопасности

- Confidentiality (Конфиденциальность): защита от несанкционированного доступа.
- Integrity (Целостность): гарантирует, что данные не изменены без разрешения.
- Availability (Доступность): обеспечивает доступ к данным при любых сбоях..

Защищает компанию от внешних угроз – утечек, шпионажа, взломов, вирусов

Использует шифрование, контроль доступа, аудит действий, резервное копирование

Предотвращает компрометацию и потерю данных

Формирует технический щит компании

CasPlan

Кибернетика

MaxPlan Solutions

Data Governance и доверие к данным

Шесть измерений качества данных (Data Quality Dimensions)

- Accuracy (Точность) – данные отражают реальность без ошибок и искажений.
- Completeness (Полнота) – присутствуют все необходимые значения и поля.
- Consistency (Согласованность) – данные совпадают во всех источниках и системах.
- Validity (Валидность) – данные соответствуют форматам и бизнес-правилам.
- Uniqueness (Уникальность) – отсутствуют дубли и повторяющиеся записи.
- Timeliness (Актуальность) – данные обновлены и доступны в нужный момент.

CasPlan

Кибернетика

MaxPlan Solutions

Основные угрозы корпоративным данным

В 2024 году число утечек данных значительно увеличилось.

Ресурсный центр по борьбе с кражей личных данных (ITRC) сообщил о 1571 крупном случае компрометации данных, затронувших около 1,07 миллиарда человек.

Число жертв утечек данных увеличилось на 490 % по сравнению с 2023 годом. Больший рост взломов отмечен в секторе финансовых услуг – увеличение на 67 %.

В 2024 году средняя стоимость утечки данных для компаний составила почти **5 миллионов долларов**, что на 10 % больше, чем в предыдущем.

- Ошибки в конфигурации облачных хранилищ и общедоступных баз данных
- Слабые пароли и дублирование пароля на разных сервисах
- Фишинговые атаки
- Ошибки и невнимательность сотрудников
- Потеря или воровство устройств
- Намеренное раскрытие информации инсайдерами
- Технические проблемы с оборудованием и системами питания
- Вредоносное ПО, программы-шифровальщики и другие причины

CasPlan

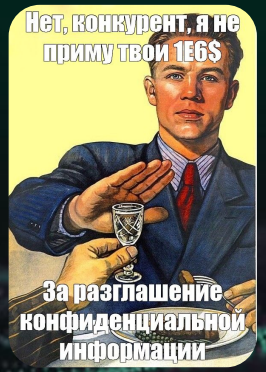
Кибернетика

MaxPlan Solutions

Типы угроз информационным активам

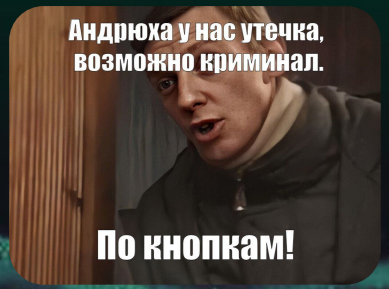
Разглашение

Намеренная или непреднамеренная передача информации недопущенным лицам



Утечка

Бесконтрольный выход информационного актива за пределы контура безопасности предприятия



Несанкционированный доступ

Противоправные действия недопущенных лиц, направленные на ознакомление с охраняемой информацией или на нарушение её целостности

CasPlan

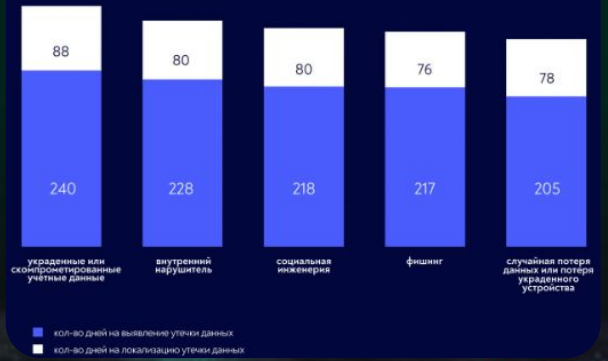
Кибернетика

MaxPlan Solutions

Стоимость рисков

277 дней
в среднем требуется на выявление и локализацию утечки данных

Топ-5:



16%
всех проникновений вызваны **фишингом**

$4.90 млн
средняя стоимость утечки данных от **инсайдерских угроз**

$4.76 млн	от **фишинга**
$4.67 млн	от **компрометации корпоративной почты**
$4.62 млн	от **украденных или скомпрометированных данных**
$4.55 млн	от **социальной инженерии**

CasPlan

Кибернетика

MaxPlan Solutions

Враг внутри: когда ошибка дороже взлома

2025

- В Астрахани сисадмин скорой помощи получил срок за установку в ритуальном агентстве ПО со сливом данным об умерших
- Атака вируса-вымогателя на медкомпанию Change Healthcare привела к утечке данных 190 млн американцев

2024

- Произошла утечка данных сотен тысяч покупателей матрасов, кроватей и постельного белья в российском магазине Spim.ru
- Произошла утечка данных сотен тысяч пользователей интернет-аптеки «Максавит»
- Произошла утечка данных миллионов пользователей российской интернет-аптеки "АптекиПлюс"
- В интернет выложили 2,7 Тбайт данных американских пациентов. Теперь у них вымогают деньги
- 400 Гбайт данных лондонских пациентов оказались в открытом доступе, потому что больницы не захотели платить выкуп
- Из-за взлома компании по управлению рецептами на лекарства произошла утечка данных 2,8 млн американцев
- **Минздрав США официально подтвердил утечку медицинских данных 55% населения страны из-за кибератаки на медкомпанию**

2023

- Произошла утечка данных сотен тысяч клиентов сети медицинских лабораторий «ЛабКвест»
- Ошибка в таблицах Excel привела к утечке данных беременных и онкобольных
- У Fresenius Medical Care в результате кибератаки украли данные 0,5 млн пациентов и сотрудников
- Один из крупнейших в мире поставщиков медизделий Henry Schein на месяц отключил свои сервисы по всему миру из-за мощной кибератаки
- В открытый доступ попала база данных пациентов клиники «РЖД-Медицина»
- Взлом генетического сервиса 23andMe: На продажу выставлена полная информация о ДНК миллионов пользователей
- Медицинская ИТ-платформа Johnson & Johnson взломана хакерами. Они получили доступ к данным пациентам с серьезными заболеваниями
- Из-за дыры в ПО IBM произошла одна из крупнейших утечек медицинских данных американцев
- Произошла утечка данных десятков тысяч клиентов сети медлабораторий KDL
- Произошла утечка данных миллионов клиентов сети медлабораторий «Хеликс»
- HCA Healthcare призналась в утечке данных 11 млн пациентов и рассказала, как она произошла
- Крупнейшая утечка в истории британского минздрава. Похищено 70 Тбайт данных медработников и пациентов
- Произошла утечка данных сотен тысяч клиентов сети аптек «Вита»
- У биотех-компании Enzo Biochem украли данные клинических исследований 2,5 млн человек. Ее атаковал вирус-вымогатель
- Хакеры выложили в открытый доступ данные 8,9 млн пациентов одной из крупнейших в США сеть стоматологий, которая отказалась платить выкуп в $10 млн
- Как киберпреступники обходят антивирусы с помощью сервисов Google
- Утечка сотен тысяч клиентов сети диагностических лабораторий «Ситилаб»
- Хакеры выложили в интернет «засекреченные» документы о российской вакцине Спутник V
- Хакеры-вымогатели взломали сеть клиник и начали публиковать фото больных раком американцев в попытке получить выкуп

Доля внутренних утечек в различных отраслях: мир, 2017 г.

Кибернетика

MaxPlan Solutions

Zero Trust Model: Никому не доверяй, всё проверяй

Zero Trust – современный стандарт ИБ

OLAP реализует Zero Trust для данных через RLS и аутентификацию при каждом действии.

CasPlan

Кибернетика

MaxPlan Solutions

Многоуровневая архитектура безопасности (RLS)

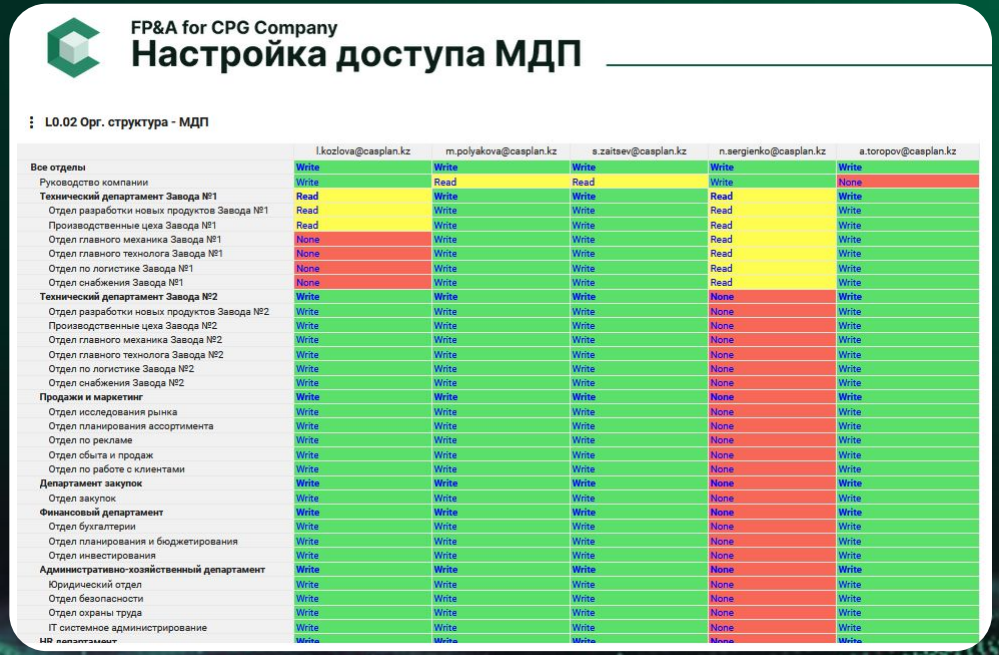
RLS – это система ограничений доступа к данным на уровне строк, позволяющая разным пользователям видеть только ту информацию, которая им разрешена, в рамках одного набора данных. Это достигается путем разделения приложения на уровни абстракции, где каждый уровень отвечает за свою функцию: логику, данные или представление.

Ключевые принципы

Ограничение доступа на уровне строк: Пользователи видят только те строки данных, которые соответствуют их правам. Например, менеджер видит данные только своего отдела, а рядовой сотрудник — только свои собственные.

Гибкость и повторное использование: Разделение на уровни позволяет вносить изменения в один слой, не затрагивая другие, что делает разработку более гибкой и повторно используемой.

Разделение функций: Приложение делится на уровни (например, уровень представления, уровень бизнес-логики и уровень хранения данных) для разделения функций и повышения безопасности.



FP&A for CPG Company

Настройка доступа МДП

L0.02 Орг. структура - МДП

	l.kozlova@casplan.kz	m.polyakova@casplan.kz	s.zaitsev@casplan.kz	n.sergienko@casplan.kz	a.toropov@casplan.kz
Все отделы	Write	Write	Write	Write	Write
Руководство компании	Write	Read	Read	Write	None
Технический департамент Завода №1	Read	Write	Write	Read	Write
Отдел разработки новых продуктов Завода №1	Read	Write	Write	Read	Write
Производственные цеха Завода №1	Read	Write	Write	Read	Write
Отдел главного механика Завода №1	None	Write	Write	Read	Write
Отдел главного технолога Завода №1	None	Write	Write	Read	Write
Отдел по логистике Завода №1	None	Write	Write	Read	Write
Отдел снабжения Завода №1	None	Write	Write	Read	Write
Технический департамент Завода №2	Write	Write	Write	None	Write
Отдел разработки новых продуктов Завода №2	Write	Write	Write	None	Write
Производственные цеха Завода №2	Write	Write	Write	None	Write
Отдел главного механика Завода №2	Write	Write	Write	None	Write
Отдел главного технолога Завода №2	Write	Write	Write	None	Write
Отдел по логистике Завода №2	Write	Write	Write	None	Write
Отдел снабжения Завода №2	Write	Write	Write	None	Write
Продажи и маркетинг	Write	Write	Write	None	Write
Отдел исследования рынка	Write	Write	Write	None	Write
Отдел планирования ассортимента	Write	Write	Write	None	Write
Отдел по рекламе	Write	Write	Write	None	Write
Отдел сбыта и продаж	Write	Write	Write	None	Write
Отдел по работе с клиентами	Write	Write	Write	None	Write
Департамент закупок	Write	Write	Write	None	Write
Отдел закупок	Write	Write	Write	None	Write
Финансовый департамент	Write	Write	Write	None	Write
Отдел бухгалтерии	Write	Write	Write	None	Write
Отдел планирования и бюджетирования	Write	Write	Write	None	Write
Отдел инвестирования	Write	Write	Write	None	Write
Административно-хозяйственный департамент	Write	Write	Write	None	Write
Юридический отдел	Write	Write	Write	None	Write
Отдел безопасности	Write	Write	Write	None	Write
Отдел охраны труда	Write	Write	Write	None	Write
IT системное администрирование	Write	Write	Write	None	Write
HR департамент	Write	Write	Write	None	Write

CasPlan

Кибернетика

MaxPlan Solutions

Audit Trail: контроль и аудит

Аудиторский след (audit trail) – это хронологическая запись всех действий и изменений данных в системе, которая фиксирует, кто, что и когда сделал. Он используется для обеспечения безопасности, подотчетности и соответствия требованиям, позволяя отслеживать историю событий, проверять точность данных, выявлять мошенничество и проводить расследования инцидентов.

Как работает аудиторский след

- Запись событий: Фиксирует каждое действие, например, вход пользователя, изменение данных, создание или удаление записи.
- Временные метки: Каждая запись снабжена точной отметкой даты и времени.
- Идентификация пользователя: Указывает, какой пользователь выполнил действие.
- Отслеживание изменений: Позволяет проследить, как менялись данные с течением времени.

CasPlan Кибернетика MaxPlan Solutions

Итоги и вывод

IBP-системы вроде Casplan меняют саму философию безопасности:

- защита не добавляется к модели, она в неё встроена.
- доверие и контроль данных не мешают бизнесу, а делают его устойчивым.
- Data Governance становится таким же важным, как финансы и продажи.

OLAP = архитектура доверия.

CasPlan Кибернетика MaxPlan Solutions

CasPlan

Спасибо за внимание!

casplan.tech

Кибернетика

MaxPlan Solutions